TASMANIA
LAW REFORM
INSTITUTE

Review of Privacy Laws in Tasmania

FINAL REPORT NO 33

MAY 2024

https://www.utas.edu.au/law-reform/publications/completed-law-reform-projects

Cite as: Tasmania Law Reform Institute, *Review of Privacy Laws in Tasmania* (Final Report No 33, May 2024)

Contents

About the Tasmania Law Reform Institute

The Tasmania Law Reform Institute is Tasmania's peak independent law reform body. The Institute was established on 23 July 2001 by agreement between the Government of the State of Tasmania, the University of Tasmania and The Law Society of Tasmania. The creation of the Institute was part of a Partnership Agreement between the University and the State Government signed in 2000. The Institute is based at the Sandy Bay campus of the University of Tasmania within the Faculty of Law. The Institute undertakes law reform work and research on topics proposed by the Government, the community, the University and the Institute itself.

The work of the Institute is to conduct impartial and independent reviews or research on areas of law and legal policy in order to provide independent and impartial advice and recommendations on the area investigated, with a view to, or for the purposes of:

i. the modernisation of the law; and/or

ii. the elimination of defects in the law; and/or

iii. the simplification of the law; and/or

iv. the consolidation of any laws; and/or

v. the repeal of laws that are obsolete or unnecessary; and/or

vi. adopting new or more effective methods for administering the law and dispensing justice; and/or

vii. providing improved access to justice; and/or

viii. uniformity between laws of other states, territories and the Commonwealth; and/or

ix. the codification of laws; and/or

x. promoting equality before the law.

The Institute's Director is Professor Jeremy Prichard of the University of Tasmania (appointed by the Vice-Chancellor of the University of Tasmania). The members of the Board of the Institute are: Craig Mackie (Chair, appointed by the Tasmanian Bar Association), Professor Gino Dal Pont (Interim Dean of the Faculty of Law at the University of Tasmania), the Honourable Justice Helen Wood (appointed by the Honourable Chief Justice of Tasmania), Kristy Bourne (appointed by the Attorney-General), Rohan Foon (appointed by the Law Society), Ann Hughes (appointed at the invitation of the Board), Kim Baumeler (appointed at the invitation of the Board), Dr Yvette Maker (Appointed by Council of University) and Rosie Smith (appointed at the invitation of the Board as a member of the Tasmanian Aboriginal community).

The Board oversees the Institute's research, considering each reference before it is accepted, and approving publications before their release.

Acknowledgements

This Inquiry was initiated by the Honourable Meg Webb, Independent member of the Tasmanian Legislative Council (see Background and Terms of Reference on pages 1–2) and funded by the Solicitors Guarantee Fund under a grant provided to the Tasmanian Law Reform Institute.

This Final Report was prepared for the Board by Dr Yvette Maker and Dr Rebecca Bradfield. Penelope Stevenson provided research assistance.

The Issues Paper that preceded this Report and informed much of its content was prepared for the Board by Daniel Stewart, Damian Clifford and Jelena Gilgorijevic, Dr Brendan Gogarty and Chun Yu, with Ms Yu also providing research assistance. The Issues Paper was edited and prepared for publication by Dr Nina Hudson.

Ongoing administrative and management of the Inquiry has been provided by Ms Kira White. This Final Report was edited and prepared for publication by Dr Jacqueline Fox.

The TLRI wishes to thank all those who made submissions in response to the questions asked in the Issues Paper. All submissions were taken into account in formulating those recommendations.

An electronic copy of the Final Report is available at the TLRI website.

An electronic copy may also be obtained by:

Email: law.reform@utas.edu.au

Phone: (03) 6226 2069

Post: Tasmania Law Reform Institute

Private Bag 89 Hobart TAS 7001

Ethical Conduct of Research

This project has been approved by the Tasmanian Social Sciences Human Research Ethics Committee. If you have concerns or complaints about the conduct of this study, please contact the Executive Officer of the University of Tasmania Human Research Ethics Committee on +61 3 6226 6254 or email human.ethics@utas.edu.au. The Executive Officer is the person nominated to receive complaints from research participants. You will need to quote ethics reference number H0016752.

Executive Summary

This Final Report consolidates the Institute's research and consideration of community and stakeholder consultation on the regulation of privacy in Tasmania. The Report follows the release of an Issues Paper by the Institute in March 2023.

This Final Report makes 63 recommendations for reforms to Tasmanian law to provide better privacy protection given the rapid advances in information technology, changing community perceptions about the importance of privacy, and growing legislative regulation of various matters. The reforms are also aimed at providing greater clarity and certainty in relation to privacy obligations to facilitate compliance by information custodians and greater awareness within the community.

As with the Issues Paper, the Final Report adopts a broad working definition of privacy ([2.2]) which covers the overlapping categories of information privacy, privacy of communications, bodily privacy, and territorial privacy. Bodily and territorial privacy are collectively known as 'rights to seclusion', which is the right to have one's physical self and one's environment free from intrusion.

Currently, there is no comprehensive privacy regulation in Tasmania. Rather, privacy protection is fragmented across different laws that protect different types of privacy in different specific circumstances ([2.5]). Different legislation may interact to affect privacy protections (Part 2). The applicability of regulations at the Australian federal level under the Privacy Act and the international level create further complexity in the landscape of privacy protection. Accordingly, in answer to the overarching question guiding this project, the TLRI's view is that existing privacy laws in Tasmania are not adequately protective.

In contemplating appropriate reforms, the TLRI considers that consistency of the Tasmanian information privacy legislation with the Commonwealth and other State and Territory legislation is desirable. This is a key issue identified in reviews elsewhere in Australia, and in submissions to this Final Report. Consistency reduces confusion, promotes information sharing and enables Tasmania to learn from the experiences in other jurisdictions.

A statutory tort for serious invasions of privacy (see Part 11)

In addressing the gaps in privacy protection, together with the fragmented landscape of protection under both legislation and general law, the TLRI considers that there is a case for creating a civil statutory cause of action (and remedy) for certain interferences with privacy. The TLRI considers that the introduction of a statutory tort for serious invasions of privacy would address a significant gap in privacy protection in Tasmania that appears unlikely to be addressed in common law in the immediate term. This view is consistent with recommendations of multiple national and State-based reviews in recent years.

A statutory tort to be enacted in a standalone Commonwealth Act, with cross-vesting of federal jurisdiction, would be the most appropriate way to introduce such a protection. However, the TLRI considers that, if the Commonwealth does not adopt the proposal of the ALRC and the Privacy Act Review in the near future, further consideration should be given to the introduction of Tasmanian legislation to create a statutory civil cause of action, or statutory tort, of privacy.

Personal Information Protection Act 2004 (Tas) (see Parts 3–8)

The primary privacy framework in Tasmania is the *Personal Information Protection Act 2004* (Tas) ('PIPA'), which binds government agencies and their contractors. It protects government-held information, primarily through prescribing 10 'Personal Information Protection Principles' ('PIPPs') by which the entities must abide. While a detailed piece of legislation, there are multiple gaps in its

scope, operation, and enforcement that can jeopardise privacy. To address these gaps, the TLRI makes recommendations relating to the scope of the information protected by:

- amending the definition of personal information;
- inserting into the PIPA a non-exhaustive list of circumstances to which PIPA personal information custodians will be expected to have regard in assessing whether identity is 'reasonably identifiable';
- inserting a definition of 'de-identified'; and
- aligning the definition of 'sensitive information' by adding biometric information and genetic information about an individual that is not otherwise health information to the PIPA definition (see [4.10]).

The TLRI also make recommendations about removing exemptions or exceptions under the PIPA relating to employee information and public information. Currently, these types of information receive less than the general level of legislative privacy protection (see [4.12]).

The TLRI also considers that a definition of law enforcement information should be included in the PIPA and that the Ministerial exemption mechanism based on a public benefit assessment in the PIPA should be amended. Further, it is the TLRI's view that exemptions for information handling in emergency situations should be provided for in the PIPA (see [4.15]).

In addressing the alignment of the Tasmanian privacy principles with the Commonwealth Act, the TLRI recommends a number of changes to the PIPPs and other provisions of the PIPA to enhance consistency and clarity for both individuals and personal information custodians and to respond more comprehensively to privacy risks associated with the increasing proliferation and sophistication of digital technology (see Parts 5–7). These reforms are in the areas of the collection, use and disclosure of personal information, data quality, security, access and correction, and complaints, monitoring, and enforcement (see Parts 5 and 6).

The TLRI notes the concerns raised in multiple submissions about the privacy risks associated with emerging technology, such as facial recognition and automated decision-making. The TLRI agrees with the findings of the Commonwealth Privacy Act Review and other recent projects (such as the AHRC's *Human Rights and Technology* project) that the risks associated with these technologies justify reforms to privacy legislation. There is considerable scope to strengthen the PIPA complaints process, and to make provision for remedies for breaches of the PIPA, in order to enhance privacy protections for individuals and foster personal information custodians' compliance with the PIPA. The TLRI considers that strengthened data breach notification measures should be implemented in Tasmania; this is discussed in more detail in Part 8. Additional resources would need to be made available to assist personal information custodians to comply with data breach notification requirements.

Other legislative provisions outside the Personal Information Protection Act 2004 (Tas) ('PIPA') that impact the privacy of government-held information

Rights relating to the handling of personal information and the right to information held by government agencies are closely related. Yet, unlike in other jurisdictions, there is a lack of clarity as to the relationship between the privacy protections in the PIPA and freedom of information rights in the *Right to Information Act 2009* (Tas) ('RTI Act'). There is also uncertainty regarding the interaction of the PIPA with other legislative schemes that have provisions restricting the sharing of government-held information or providing for access to information. Accordingly, it is the TLRI's view that there should be a close examination of the relationship between the provisions of the PIPA and other Tasmanian legislation with a view to obtaining greater harmonisation and consistency between them (see Part 9).

Other legislation provides protection against multiple forms of harm to privacy interests but these are generally limited to activities or circumstances in which specific interferences with privacy might occur. These include stalking, harassment, image-based abuse (previously called 'revenge pornography'), governmental or workplace surveillance, and handling of health information.

In relation to the issue of the adequacy of the surveillance legislation applying in Tasmania ([10.2]–[10.11]), the TLRI notes that generally the approach under the *Listening Devices Act 1991* (Tas) and the *Police Offences Act 1935* (Tas) provides a broad safeguard for individual privacy. Nevertheless, the TLRI considers that there is scope to expand existing surveillance protections contained in the *Listening Devices Act 1991* (Tas) to cover a broader range of technologies, such as visual and tracking devices, as exists in most other jurisdictions.

Stalking, harassment, and bullying may in some circumstances involve interference with privacy—whether through intrusion upon seclusion (also referred to as physical privacy, meaning a person's bodily or territorial privacy) or through the malicious use of private information against the person concerned (for example, to intimidate, blackmail, or otherwise coerce that person). As with other egregious interferences with privacy, these behaviours may cause humiliation, psychological distress, or intimidation.

After reviewing the legislation that exists in other jurisdictions, and taking into account the submissions received, the TLRI's view is that there are areas in which the laws that apply in relation to stalking and bullying could be strengthened in Tasmania to provide greater clarity around, and better protection for, physical privacy. There is also a need to enact State-based offences relating to distributing an intimate image without consent or threatening to distribute an intimate image. This is consistent with the *National Statement of Principles relating to the Criminalisation of the Non-consensual Sharing of Intimate Images*, which sets out principles for nationally consistent criminal offences.

Recommendations

Recommendation 1: The definition of 'personal information' in the PIPA should be amended to:

- replace 'about' with 'relating to'; and
- introduce a non-exhaustive list of information that may fall within the definition of personal information.

Recommendation 2: Further consideration should be given to:

- amending the definition of 'personal information' by replacing 'reasonably ascertainable' with 'reasonably identifiable'; and
- providing further guidance for personal information custodians by inserting a non-exhaustive list of circumstances to which PIPA personal information custodians will be expected to have regard in assessing whether identity is 'reasonably identifiable'.

Recommendation 3: The PIPA should be amended to insert a definition of 'de-identified' that is consistent with the definition in the *Privacy Act 1988* (Cth) and that clarifies that 'de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context'.[1]

Recommendation 4: Further consideration should be given to whether the PIPA should be amended to:

- introduce a criminal offence for 'malicious re-identification' of de-identified information where there is an intention to harm or obtain an illegitimate benefit;[2] and/or
- introduce a prohibition on PIPA personal information custodians from re-identifying information obtained from a source other than the individual to whom the information relates.[3]

Recommendation 5: The definition of 'sensitive information' in the PIPA should be amended to include:

- biometric information used for the purpose of automated biometric verification or biometric identification;
- biometric templates; and
- genetic information about an individual that is not otherwise health information.

Recommendation 6: If Recommendation 1 is implemented, the definition of 'sensitive information' should also be amended to replace 'about' with 'relating to'.

Recommendation 7: The definition of 'health information' in the PIPA should be amended to align with the definition of 'personal information'.

Recommendation 8: In line with developments at the Commonwealth level and the desirability of consistency with the approach in other jurisdictions, further consideration should be given to amending the PIPA to expand the definition of 'sensitive information' to:

- include genomic information; and
- include inferences about sensitive information.

[1] Privacy Act Review Report 2022 Proposal 4.5.
[2] Ibid Proposal 4.7.
[3] Ibid Proposal 4.8.

Recommendation 9: Pending the outcome of the Commonwealth Privacy Act Review, further consideration should be given to amending the PIPA to:

- insert a definition of geolocation tracking data; and
- specify that such geolocation tracking data can only be collected, used, disclosed, and stored with consent.

Recommendation 10: Section 12 of the PIPA should be subject to further consultation with public authorities, to clarify whether the provision is necessary in light of other information-sharing provisions in the PIPA.

Recommendation 11: The employee information exemptions in the PIPA should be removed.

Recommendation 12: The public information exemption in the PIPA should be removed. Consideration should be given to ensuring that appropriate resources, guidance and transition periods are set to enable public authorities to comply with this amendment.

Recommendation 13: A definition of 'law enforcement information' should be included in the PIPA.

Recommendation 14: The public benefit exemption mechanism should be amended to either:

(a) introduce a mechanism making Ministerial public benefit determinations subject to disallowance by the Parliament; or
(b) if Recommendation 47 is adopted and an independent office-holder (such as an information commissioner or a privacy commissioner) is established, confer the power to make public benefit determinations on that office-holder, subject to disallowance by the Parliament.

Recommendation 15: There should be appropriate exemptions for information handling in emergency situations in the PIPA.

Recommendation 16: The term 'collects' should be defined in the PIPA, and the definition should include inferred and generated information.

Recommendation 17: PIPP 1(3) should be amended to require personal information custodians to disclose who else may have access to the information once collected.

Recommendation 18: PIPP 1 should be amended to require personal information custodians to take reasonable steps to give notice of collection at or before the time of collection or, if that is not practicable, as soon as practicable after collection.

Recommendation 19: Further consideration should be given to the recommendations of the Commonwealth Privacy Act Review in relation to whether the PIPA requirements relating to collection notices should be amended to:

- require that collection notices should be clear and understandable (including where addressed to a child) and accessible; and
- require that collection notices contain additional details, such as details of the circumstances of handling where a high-risk activity is involved, information about the privacy policy and what it contains, and information about individual rights and types of information that may be disclosed to cross-border recipients.

Recommendation 20: PIPP 1 should be amended to enable personal information custodians to collect personal information about an individual from a person other than the individual, where the individual has consented or the custodian is required by law to collect the information.

Recommendation 21: The PIPA should be amended to insert a definition of 'consent' consistent with the definition of valid consent in the OAIC Guidelines on the Australian Privacy Principles.

Recommendation 22: Guidance on the design of consent requests for online services should be available to personal information custodians.

Recommendation 23: PIPP 1 should be amended to specify how personal information custodians should respond to receiving unsolicited information.

Recommendation 24: Further consideration should be given to aligning the PIPA with the Privacy Act in relation to cross-border in terms of:

- whether personal information custodians should be required to hold a reasonable belief that there are mechanisms for the individual to enforce existing privacy protections prior to cross-border disclosure;
- whether personal information custodians should be required to expressly inform individuals that, if the individual consents to cross-border disclosure, the custodian will not be obliged to take reasonable steps to ensure the recipient does not breach the PIPP (and, per the Privacy Act Review's further proposal, that privacy protections may not apply to the recipient); and
- whether personal information custodians retain responsibility for breaches of the PIPPs after they have taken reasonable steps to ensure the recipient deals with the information consistently with the PIPPs.

Recommendation 25: The PIPA should be amended to include a definition of 'disclosure' consistent with the current definition in the OAIC Guidelines on the Australian Privacy Principles.

Recommendation 26: The PIPA should be amended to require that collection, use and disclosure of personal information must be fair and reasonable in the circumstances, in line with the recommendation of the Privacy Act Review.[4]

Recommendation 27: The PIPA (PIPP 1) should be amended to require personal information custodians to determine and record the purposes of collection, use, and disclosure of personal information, including any secondary uses or disclosures.

Recommendation 28: The scope of PIPA information handling exceptions relating to requirement or authorisation under law should be clarified.

Recommendation 29: The PIPA should be amended to state that consent to personal information handling must be 'voluntary, informed, current, specific, and unambiguous', in line with the proposal of the Privacy Act Review.

Recommendation 30: The Tasmanian Government should participate in cross-jurisdictional work on the scope and harmonisation of research exceptions in privacy legislation (as proposed by the Privacy Act Review), including in relation to the introduction of a 'broad consent' option for research-related personal information handling.

Recommendation 31: Further consultation with stakeholders, including children and young people and their parents and carers, should be undertaken to ensure that privacy protections under the PIPA are appropriate for children and young people and are consistent with contemporary understandings of children's decision-making capacity. Matters for consultation may include:

- whether the PIPA should be amended to specify that consent to information handling will only be valid where the individual has capacity to consent;

[4] Privacy Act Review Report 2022 Proposals 12.1, 12.2, 12.3.

- whether the PIPA should be amended to establish exceptions to consent requirements where seeking consent from a parent or guardian would be inappropriate or harmful for the child or young person; and
- whether guidance should be developed to assist personal information custodians to assess the capacity of children and young people on a case-by-case basis.

Recommendation 32: Guidance on capacity and consent, including guidance on recognising and facilitating supported decision-making, should be available to personal information custodians.

Recommendation 33: An individual 'right to object', with the same features as the right proposed by the Commonwealth Privacy Act Review, should be introduced in the PIPA.

Recommendation 34: PIPP 4 should be amended, in line with the corresponding proposals of the Commonwealth Privacy Act Review, to:

- provide further guidance to personal information custodians on the 'reasonable steps' they must take to protect personal information;
- set baseline privacy outcomes personal information custodians must meet to fulfil their data security obligations; and
- require personal information custodians to set and periodically review retention periods for personal information.

Recommendation 35: Consideration should be given to whether further guidance on PIPA-compliant destruction and de-identification of personal information by personal information custodians, similar to the revised guidance proposed by the Commonwealth Privacy Act Review, is necessary.

Recommendation 36: An individual 'right to erasure', with the same features as the right proposed by the Commonwealth Privacy Act Review, should be introduced in the PIPA.

Recommendation 37: There should be a review of all Tasmanian legislation that requires retention of personal information to ensure it appropriately balances policy objectives and privacy and cyber-security risks.

Recommendation 38: PIPP 6 should be amended to require a personal information custodian to:

- provide individuals with access to their personal information upon request;
- provide access to personal information in the manner requested by the individual, as long as this is reasonable and practicable, without charge;
- give written notice of the reasons for a refusal to give access and the mechanisms available to complain about the refusal (which are discussed further in Part 8 of this Report); and
- adopt a presumption in favour of disclosure.

Recommendation 39: PIPP 6 should be amended to simplify the process for requesting access to personal information. These amendments should clarify the interaction of the PIPA and the RTI Act.

Recommendation 40: PIPP 6 should be amended to confer an individual right to explanation about personal information, including a right to explanation of the source of personal information collected indirectly, and a right to an explanation or summary of what a personal information custodian has done with the personal information.[5]

Recommendation 41: Part 3A of the PIPA should be amended to:

[5] See Privacy Act Review Report 2022 Proposal 18.1.

- modify the operation of Section 17G to enable a person to request (rather than require) the personal information custodian to add information to a notation;
- require a personal information custodian to provide a written notice of a refusal of a request to add information to a notation; and
- extend the right to correction in Section 17A to enable persons to request amendment of incorrect, incomplete, out-of-date or misleading information in generally available publications online over which a personal information custodian maintains control.

Recommendation 42: Individual rights to access and explanation, to object, to erasure, and to correction in the PIPA should be subject to the exceptions proposed by the Commonwealth Privacy Act Review; namely, where:

- there are competing public interests;
- required or authorised by law or legal relationships; and
- technically infeasible or an abuse of process.

Recommendation 43: Personal information custodians should be required to provide 'reasonable assistance' to individuals in exercising a right, take 'reasonable steps' to respond to an exercise of a right, and respond within a prescribed timeframe, unless a longer period is justified.

Recommendation 44: There should be greater clarity around how personal information custodians should meet the requirements of PIPP 5. This should include:

- specifying the type of information that must be included in privacy policies made under PIPP 5; and
- requiring personal information custodians to designate a senior employee as privacy officer responsible for compliance with the PIPA.

This could be implemented by amendment to legislation or regulation, or the development of guidelines.

Recommendation 45: The PIPA should be amended to:

- require personal information custodians to specify the types of personal information that will be used in automated decision-making; and
- establish a right to request meaningful information about how such decisions are made.

Recommendation 46: Guidance should be developed to support personal information custodians to meet new requirements relating to automated decision-making.

Recommendation 47: Consideration should be given to:

- the most appropriate form that a body responsible for broadened enforcement and compliance functions under the PIPA should take; and
- ensuring adequate resourcing for that body.

Recommendation 48: Consideration should be given to the introduction of a requirement for the Ombudsman (or other complaints-handling body) to consider the appropriateness of conciliation when dealing with a complaint. There should also be jurisdiction for TasCAT to hear a complaint if the Ombudsman (or other complaints-handling body) decides that it is not reasonably possible that a complaint be conciliated successfully.

Recommendation 49: Community consultation should be undertaken to ensure that changes to complaints and review processes under the PIPA are available and accessible to all in the community.

Recommendation 50: Decisions of the Ombudsman (or other complaints-handling body) in relation to PIPA complaints should be reviewable by TasCAT.

Recommendation 51: TasCAT should be empowered to make appropriate orders against personal information custodians, where all or part of a PIPA complaint has been proven.

Recommendation 52: Consideration should be given to strengthening the enforcement regime through:

- the creation of offences for certain conduct;
- a civil penalty regime; and/or
- the creation of additional enforcement mechanisms such as injunctions and enforceable undertakings.

Guidance can be sought from the provision in other Australian jurisdictions as to the scope of the regimes.

Recommendation 53: The power of the Ombudsman (or other complaints-handling body) to conduct investigations into breaches of the PIPPs, regardless of whether a complaint has been received, should be clarified.

Recommendation 54: The PIPA should be amended to enable the creation of privacy codes.

Recommendation 55: The TLRI recommends that Tasmania introduce a data breach notification scheme based on the Commonwealth model.

Recommendation 56: There should be a close examination of the relationship between the provisions of the PIPA and other Tasmanian legislation with a view to obtaining greater harmonisation and consistency between them. In this review, there is a need to ensure privacy protection is maximised to the extent that is possible in balance with other policy interests.

Recommendation 57: The Tasmanian Government should undertake a review of provisions that present legislative barriers to the sharing of information within government and with relevant non-government organisations in the interests of protecting the safety and wellbeing of children and young people, people in family violence situations, abuse of elder persons and people with disabilities.

Recommendation 58: Consideration should be given to reform of the listening devices legislation to strengthen protections for individuals against surveillance by optical surveillance devices, tracking devices, and data surveillance devices.

Recommendation 59: Consideration should be given to improving the resources made available to allow for independent monitoring of police use of surveillance devices by the Ombudsman.

Recommendation 60: A review should be conducted that examines the adequacy of the existing laws relating to stalking and intimidation in Tasmania and that considers whether there is a need to amend these laws to take better account of technological advances. The following could be considered in the review:

- whether the crime of stalking and bullying in the *Criminal Code* (Tas) Section 192 should be amended to include intimidation based on the New South Wales approach—with intimidation being defined separately from stalking—and the provision should be changed to recognise that a single act, or a pattern of behaviour, may be taken into account in the determination of stalking or intimidation;
- the extent to which behaviour that amounts to harassment is adequately protected for the purposes of the *Family Violence Act 2003* (Tas); and
- whether the crime of stalking and bullying in the *Criminal Code* (Tas) Section 192 should be amended to more clearly criminalise surveillance conducted by technology; for example, by

installing tracking and spyware applications on mobile phones, electronic devices, and vehicles, as well as installing covert cameras and the use of drones.

Recommendation 61: Tasmania should, in line with other jurisdictions, enact state-based legislation to create offences of distributing an intimate image without consent or threatening of distribute an intimate image. In the creation of such an offence, the law should make it clear that the prohibition extends to the distribution (or threat to distribute) images created or modified by the use of artificial intelligence.

Recommendation 62: There should be further consideration of necessary reforms to the PIPA, or the creation of standalone legislation, to align Tasmanian regulation with the *National Health Interoperability Plan*.

Recommendation 63: If a national statutory tort is not adopted by the Commonwealth in the near future, consideration should be given to the introduction of Tasmanian legislation to create a statutory tort of privacy.

List of Acronyms and Abbreviations

In this Final Report, language that is consistent with relevant Acts is used wherever possible. The following is a list of the most frequently used acronyms, abbreviations, and key terms.

2017 APP Code	*Privacy (Australian Government Agencies – Governance)* APP Code 2017
AAT	Administrative Appeals Tribunal
ACCC	Australian Competition & Consumer Commission
ACT	Australian Capital Territory
ADEPT	Administrative Data Exchange Protocol for Tasmania
ADM	automated decision-making
AHRC	Australian Human Rights Commission
AI	artificial intelligence
ALRC	Australian Law Reform Commission
APPs	Australian Privacy Principles
APRA	Australian Prudential Regulation Authority
ASIC	Australian Securities and Investments Commission
CCTV	closed circuit television
CDR	Consumer Data Right
CoI	Commission of Inquiry into the Tasmanian Government's Responses to Child Sexual Abuse in Institutional Settings
CRC	United Nations Committee on the Rights of the Child
HRIP Act (NSW)	*Health Records and Information Privacy Act 2002* (NSW)
ICCPR	*International Covenant on Civil and Political Rights*
IP Act (Qld)	*Information Privacy Act 2009* (Qld)
IPA (ACT)	*Information Privacy Act 2014* (ACT)
FOI Act	*Freedom of Information Act 1982* (Vic)
FRT	facial recognition technology
GDPR	European Union *General Data Protection Regulation 2016/679*
HCC	Health Complaints Commission
Health Complaints Act	*Health Complaints Act 1995* (Tas)

MLC	Member of the Legislative Council
MNDB	Mandatory Notification of Data Breach Scheme (NSW)
NDLFRS	National Driver Licence Facial Recognition Solution
NHMRC	National Health and Medical Research Council
NSWPC	New South Wales Privacy Commissioner
OAIC	Office of the Australian Information Commissioner
OVIC	Office of the Victorian Information Commissioner
PDPA (Vic)	*Privacy and Data Protection Act 2014* (Vic)
PIPA	*Personal Information Protection Act 2004* (Tas)
PPIP Act (NSW)	*Privacy and Personal Information Protection Act 1998* (NSW)
Privacy Act	*Privacy Act 1988* (Cth)
PIPPs	Personal Information Protection Principles
QCAT	Queensland Civil and Administrative Tribunal
QIC	Queensland Information Commissioner
QPP	Queensland Privacy Principles
RPA	Remotely Piloted Aircraft (drones)
RTI Act	*Right to Information Act 2009* (Tas)
SALRI	South Australia Law Reform Institute
TasCAT	Tasmanian Civil and Administrative Tribunal
TasCOSS	Tasmanian Council of Social Service
TLA	Tasmanian Legal Aid
TLGC	Tasmanian Liquor and Gaming Commission
TLRI	Tasmania Law Reform Institute
ToRs	Terms of Reference
UAV	Unmanned Aerial Vehicles (drones)
VCAT	Victorian Civil and Administrative Tribunal
VIC	Victorian Information Commission
YLA	Youth Law Australia

Part 1

About this Final Report

1.1 Background

1.1.1 This Final Report consolidates the Tasmania Law Reform Institute's research and consideration of community and stakeholder consultation on the regulation of privacy in Tasmania. The Report follows the release of an Issues Paper by the Institute in March 2023.

1.1.2 The Inquiry into Privacy Laws in Tasmania was initiated by the Honourable Meg Webb, Independent member of the Tasmanian Legislative Council. The Reference was accepted by the Tasmanian Law Reform Institute ('TLRI') Board in December 2019. The TLRI applied for a grant from the Solicitors Guarantee Fund to undertake the Inquiry. In May 2020, the TLRI received advice that its application had been partially successful, with a lesser amount granted than requested.

1.1.3 The issue of privacy protection is topical in view of the matters raised in the Terms of Reference below, as well as other developments, such as several high-profile, national data breaches relating to organisations such as Medicare and Optus, and the Commonwealth's comprehensive Review of the *Privacy Act 1988* (Cth), which concluded with the publication its final report in February 2023.

1.1.4 The Terms of Reference were referred to the TLRI in view of:

- the rapid and extensive advances in information, communication, storage, surveillance and other relevant technologies;
- possible changing community perceptions of privacy and the extent to which it should be protected by legislation;
- the expansion of state and territory legislative activity in relevant areas; and
- emerging areas that may require privacy protection.

1.1.5 The TLRI acknowledges that defining the scope of privacy has proved an 'elusive task',[6] and it has been described through several typologies or categories. In responding to the Terms of Reference, the TLRI has adopted a definition of privacy that is consistent with definitions adopted in other jurisdictions and other recent law reform reviews (discussed at [2.2]).

1.2 Terms of Reference

1.2.1 The Terms of Reference for this project were:

for the TLRI to inquire into, review and report on:

[6] Australian Law Reform Commission ('ALRC'), *Privacy* (Report No 22, 1983).

- the current protections of privacy and of the right to privacy in Tasmania and any need to enhance or extend protections for privacy in Tasmania;
- the extent to which the *Personal Information Protection Act 2004* (Tas) and related laws continue to provide an effective framework for the protection of privacy in Tasmania and the need for any reform to that Act; and
- models that enhance and protect privacy in other jurisdictions (in Australia and overseas).

in undertaking this reference, for the TLRI to consider and have regard to:

(a) the United Nations *International Convention on Civil and Political Rights* and other relevant international instruments that protect the right to privacy;

(b) relevant existing and proposed Commonwealth, state and territory laws and practices;

(c) any recent reviews of the privacy laws in other jurisdictions;

(d) current and emerging international law and obligations in this area;

(e) privacy regimes, developments and trends in other jurisdictions;

(f) the need of individuals for privacy protection in an evolving technological environment; and

(g) any other related matter.

for the TLRI to identify and consult with relevant stakeholders and ensure widespread public consultation on how privacy and obligations relating to protecting privacy can best be promoted and protected in Tasmania and provide recommendations as to an appropriate model for Tasmania to protect and enhance privacy rights and protections.

1.3 Conduct of Inquiry

1.3.1 Following the acceptance of the reference by the TLRI Board, Institute and external researchers worked throughout 2021 and 2022 to prepare an Issues Paper for community consultation. The Issues Paper was reviewed by the TLRI Board and approved in early 2023 for public release.

1.3.2 Finalisation of the Issues Paper in January 2023 preceded the public release of a report, on 16 February 2023, by the Commonwealth Attorney-General's Department on its review of the *Privacy Act 1988* (Cth) ('Privacy Act Review'). Accordingly, the Issues Paper did not consider the findings of the report as to options for reforming the *Privacy Act 1988* (Cth) ('Privacy Act') or its implications, if any, for reforming Tasmanian legislation. The proposals in the Privacy Act Review Report, and the Federal Government's response to it (published in September 2023), were considered in the preparation of this Final Report and the formulation of recommendations. In addition, on 26 September 2023, the final report of the Commission of Inquiry examining the Tasmanian Government Responses to Child Sexual Abuse in Institutional Settings was tabled in Parliament and publicly released. That report also contained recommendations relevant to the matters raised in this reference. Those recommendations are discussed at relevant points in this Report.

1.3.3 The TLRI Issues Paper:

- explained the concept of privacy protection and gave an overview of existing legal frameworks for privacy protection in Tasmania, Australia, and internationally;
- discussed the scope, operation, and enforcement of privacy protection under these privacy frameworks, focusing on information held by government agencies;

- compared the protections in Tasmania under the *Personal Information Protection Act 2004* (Tas) ('PIPA') with those in other Australian jurisdictions, particularly under the Privacy Act;
- considered possible future reforms of these frameworks and examines international developments, including the European Union's *General Data Protection Regulation 2016/679* ('GDPR');
- explored different provisions in legislation other than the PIPA that affect how government-held information can be used and shared. It analysed how these provisions affect information privacy and draws comparisons with similar laws in other jurisdictions;
- considered various types of privacy protections for information other than government-held information, under legislation and case law, such as legislation regulating information in the context of health services, legislation regulating surveillance (by government or otherwise), criminal laws which create offences relating to stalking and harassment and to the sharing of intimate images, and non-legislative protections in the general law; and
- considered the introduction of a comprehensive civil remedy for interference with privacy and the appropriate model for such a reform.

1.3.4 In discussing the strengths and weaknesses of the PIPA and privacy laws more generally, the Issues Paper sought input from the community on several issues, including whether:

- certain entities should be covered by the PIPA
- a greater range of remedies should be available for those affected by a breach of the PIPA
- a data breach notification requirement should be introduced
- new rights to object and to erasure should be introduced
- there should be privacy regulation on specific technology such as drones
- existing judicial recognition of privacy affords adequate protection, and
- there should be a civil cause of action for privacy and, if so, what its scope should be.

1.3.5 A copy of the Issues Paper can be found on the Institute's website.

1.3.6 The TLRI invited responses to the Issues Paper, either in writing (by completing the submission template provided on the TLRI website or through a more detailed written response), requesting a meeting, or attending one of several consultation roundtables arranged by the TLRI in July 2023.

1.3.7 The community consultation period took place between 2 May and 11 July 2023.

1.3.8 After the community consultation closed, Institute researchers reviewed and analysed all submissions and began preparing this Final Report. The TLRI Board provided final approval of this report and its recommendations in April 2024

1.4 Submissions to the Inquiry

1.4.1 The Institute received 21 submissions (most in writing and a small number provided verbally during meetings with Institute researchers). Of these,

- 18 were public;

- 2 were anonymous; and
- 1 was confidentially made.

1.4.2 Public submissions are listed on the TLRI website. All submissions were reviewed by at least two TLRI researchers. The Institute thanks all respondents who took the time to consider the Issues Paper and respond to its questions.

1.4.3 Consistent with the options outlined in the Issues Paper, in this Final Report, public submissions may be directly quoted or referred to and the source named. Anonymous submissions may be directly quoted or referred to but without identifying the source. Confidential submissions are not directly referred to or quoted from but are for general background and/or aggregated statistical data. Public and anonymous submissions are referenced in this Report by submission number, ordinarily in a footnote reference.

1.5 Approach of the TLRI in the Final Report

1.5.1 As noted above at [1.3.2], since the preparation of the Issues Paper, a significant review of privacy laws in Australia has been released. This has required flexibility in the approach taken by the TLRI in this Final Report. In the Issues paper, in accordance with the Terms of Reference, the TLRI examined the current scope of privacy protections in Tasmania and considered the need for any reforms that would enhance or extend those protections. The focus of the research set out in the Issues Paper and the questions asked was to obtain a high-level or broad understanding of areas of concern about gaps and shortcomings in existing privacy protections in Tasmania with a view to making recommendations for reform. The Commonwealth Privacy Act Review examined broader issues such as the need for a tort of invasion of privacy, but also provided an in-depth examination of the specific aspects of the Privacy Act and the Australian Privacy Principles (APPs) that have considerable relevance to reform to the Tasmanian PIPA and Personal Information Protection Principles ('PIPPs'). That analysis is incorporated into this Final Report and, in instances where the matter was addressed in the Issue Paper and the subject of consultation, the TLRI makes recommendations for reform. For issues where the level of detail and proposals for reform set out in Privacy Act Review were not the subject of consultation in Tasmania, and the TLRI's view is that it is not appropriate to make a recommendation for a specific reform, the issue has instead been flagged as an area for further consideration and consultation.

1.5.2 Further, in light of widespread consensus on the need for consistency in privacy regulation across Australian jurisdictions (discussed at [2.6]–[2.8]), and the significant review of the Commonwealth Privacy Act and reform proposals arising from it, the approach under the Privacy Act and proposals set out in the Commonwealth Privacy Act Review are the focus of the TLRI's discussion of the approach in other jurisdictions throughout this Final Report. The TLRI also outlines the position in other Australian jurisdictions, where appropriate.

1.5.3 This Report sets out the law until 31 January 2024. This Report is divided into Parts.

- Part 2 sets out the nature and scope of existing privacy laws in Tasmania, community attitudes to privacy, and privacy protections. It also explains the approach taken to analysing existing privacy-related laws and proposed reforms.
- Part 3 examines the scope and application of the PIPA and considers whether the PIPA, which applies broadly to Tasmanian public authorities and some government contractors, should apply to other bodies.

- Part 4 examines the scope of the PIPA in terms of the information for which it provides protection.
- Parts 5–8 address the issue of aligning the PIPPs with the Commonwealth Act in key areas such as: collection, use, and disclosure (Part 5); data quality, data security and access and correction (Part 6); openness, unique identifiers, and the option of anonymity (Part 7); and complaints, monitoring, and enforcement (Part 8). The Parts consider the similarities and differences between each of the PIPPs and the Commonwealth APPs (as they apply to government agencies) and whether reform is necessary.
- Part 9 considers necessary reforms to other legislation impacting the privacy of government-held information.
- Part 10 makes recommendations in relation to reforms in other legislation that affects privacy, such as in relation to surveillance, stalking, and image-based abuse.
- Part 11 discusses the development of the common law in Australia relating to a potential tort of interference with privacy and makes recommendation for the introduction of a statutory tort of privacy.

Part 2

Privacy Protections in Tasmania

2.1 Introduction

2.1.1 The overarching question guiding this project is whether existing privacy laws in Tasmania are adequately protective. This Part describes the nature and scope of those laws and community attitudes to privacy and privacy protections. It also explains the approach taken in this Report to analysing existing privacy-related laws and proposing reform.

2.2 Defining privacy and its importance

2.2.1 Defining the scope of privacy has proved an 'elusive task';[7] privacy is generally described using one of several typologies or categories. In its 2008 report on *Australian Privacy Law and Practice*, the Australian Law Reform Commission ('ALRC') referred to four overlapping categories of privacy protection, which have also been adopted as working definitions in this TLRI Review:

Information privacy, which involves the establishment of rules governing the collection and handling of personal data, such as credit information, medical records, and government records. It is also known as 'data protection'.

Bodily privacy, which concerns the protection of people's physical selves against invasive procedures, such as genetic tests, drug testing, and cavity searches.

Privacy of communications, which covers the security and privacy of mail, telephones, email, and other forms of communication.

Territorial privacy, which concerns the setting of limits on intrusion into the domestic and other environments, such as the workplace or public space. This includes searches, video surveillance, and ID checks.[8]

2.2.2 Rights to bodily and territorial privacy are also known as 'rights to seclusion'. Intrusions on seclusion include watching, listening to, or recording what a person does in private.[9]

2.2.3 The protection of privacy is important to individuals and society for a range of reasons, including:

[7] ALRC, *Privacy*.
[8] ALRC, *For Your Information: Australian Privacy Law and Practice* (Report No 108, August 2008) [1.31] ('*For Your Information*'), citing David Banisar, 'Privacy and Human Rights 2000: An International Survey of Privacy Law and Developments', Privacy International.
[9] ALRC, *Serious Invasions of Privacy in the Digital Era* (Report No 123, June 2014) [5.18].

- its role in safeguarding human dignity[10] and autonomy,[11] because the ability to control and choose how information about oneself is provided to others can be a precondition for individual liberty;[12]
- its role in protecting psychological well-being and security, fostering intimacy, and promoting intellectual development;[13] and
- its social benefits, which include enabling social interaction, encouraging participation in democratic processes, encouraging cultural and critical innovation, and assisting cohesion in pluralistic communities.[14]

2.3 Community attitudes to privacy and privacy protections

2.3.1 Recent survey data indicate that Australians have a relatively low level of knowledge about what current privacy protections exist, but also a belief that government should pass more laws to protect privacy.

2.3.2 In August 2023, the Office of the Australian Information Commissioner ('OAIC') released the results of a survey examining Australian Community Attitudes to Privacy.[15] The OAIC reported that, 'Australians have low awareness of privacy legislation, notably around their rights to access information organisations hold about them and organisation types that are exempt from the Australian Privacy Act'.[16] Other key findings from the survey indicate that:

- 62% of respondents see the protection of their personal information as a major concern in their life;[17]
- 90% of respondents say they have a clear understanding of why they should protect their personal information, but only 50% of respondents have clear understanding of how to protect personal information;[18]
- 69% of respondents are aware of Australian privacy law that promotes and protects the privacy of individuals,19 but only 2% of respondents correctly named the Privacy Act or Australian Privacy Principles;[20]
- 79% of respondents believe they should have the right to ask a government agency to delete their personal information;[21]

[10] Charles Fried, 'Privacy' (1968) 77(3) *Yale Law Journal* 475.
[11] Kirsty Hughes, 'A Behavioural Understanding of Privacy and Its Implications for Privacy Law' (2012) 75(5) *Modern Law Review* 806.
[12] Alan F Westin, *Privacy and Freedom* (Atheneum Press, 1967).
[13] See generally Jelena Gligorijevic, 'A Common Law Tort of Interference with Privacy for Australia: Reaffirming *ABC v Lenah Game Meats*' (2021) 44(2) *University of New South Wales Law Journal* 673, 686–7 ('Reaffirming *ABC v Lenah Game Meats*').
[14] Ibid 687.
[15] Office of the Australian Information Commissioner ('OAIC'), *Australian Community Attitudes to Privacy Survey* (2023) <https://www.oaic.gov.au/engage-with-us/research-and-training-resources/research/australian-community-attitudes-to-privacy-survey/australian-community-attitudes-to-privacy-survey-2023>.
[16] Ibid 30.
[17] Ibid 8.
[18] Ibid 16.
[19] Ibid 9.
[20] Ibid 31.
[21] Ibid 37.

- 89% of respondents believe they should be able to seek compensation in the courts for a breach of privacy;[22]
- 89% of respondents believe that government agencies should do more to protect personal information;[23] and
- 89% of respondents say they would like the government to pass more legislation that protects their personal information.[24]

2.3.3 Changes in community perceptions of the importance of privacy were also identified in the survey, which observed that there had been 'some notable shifts in Australians' awareness and attitudes towards privacy' and these were attributed to significant events such as the COVID19 pandemic, high-profile data breaches, and technical innovations in the areas of artificial intelligence and facial recognition.[25] Changes in attitudes identified in the 2023 survey, as compared to the 2020 survey, included:

- a slight increase in the number of respondents (to 21%) who claim to have 'very good or excellent' knowledge of data protection and privacy rights;[26]
- a slight increase in the number of people who say they were aware of the Australian privacy law;[27]
- a decrease in awareness of exempt organisation types;[28]
- an increase in the number of respondents who think that businesses collecting work-related information should be held to the same standard as federal government agencies and larger businesses;[29]
- an increase in the 'level of comfort with the government using personal information for research and service and policy development';[30]
- an increase in the proportion of parents who believe that 'children have the right to grow up without being profiled and targeted';[31] and
- an increase in the strength of respondents' concern about the privacy of their children.[32]

2.4 Do Tasmanians enjoy a fundamental right to privacy?

2.4.1 The *International Covenant on Civil and Political Rights*[33] ('ICCPR') declares that the right to privacy is one of the human rights held by all people worldwide. Specifically, Article 17 of the ICCPR

[22] Ibid.
[23] Ibid 41.
[24] Ibid 42.
[25] Ibid 7.
[26] OAIC, *Australian Community Attitudes to Privacy Survey* 19. It is noted that there was a disparity identified in relation to self-rated assessments (those who rated themselves as having 'very good' or 'excellent' knowledge) and the results of testing about knowledge, particular for younger Australian and males. Ibid 21.
[27] Ibid 31.
[28] Ibid.
[29] Ibid.
[30] Ibid 51.
[31] Ibid 81.
[32] Ibid 82.
[33] *International Covenant on Civil and Political Rights*, opened for signature 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976) art 17 ('ICCPR').

prohibits governments from interfering with a person's privacy and obliges governments to take positive steps to protect against interference by others.[34] It states:

> (1) No one shall be subjected to arbitrary or unlawful interference with [their] privacy, family, home or correspondence, nor to unlawful attacks on [their] honour and reputation.
>
> (2) Everyone has the right to the protection of the law against such interference or attacks.[35]

2.4.2 The right in Article 17 is not absolute and protects only against unlawful or arbitrary interference—lawful and non-arbitrary interferences are permissible. For government interference with privacy to be lawful, it must generally be authorised by legislation that details the circumstances when such government action is permitted and facilitates some form of review or accountability.[36] To be non-arbitrary, the interference must be reasonable in the circumstances. Reasonableness generally implies a test of proportionality and necessity. The interference must be proportional to the purpose of the authorising provision, and it must be necessary in the circumstances of any given case.[37]

2.4.3 Australia has signed and ratified the ICCPR, which means that it has consented to be bound to it; however, for a right under international law to be enforceable domestically, it must be introduced under Australian law.

2.4.4 As discussed further below (see [2.5.5]), privacy-specific legislation has been enacted by the Commonwealth in partial implementation of Australian's obligations under Article17. Human rights legislation in Queensland, Victoria, and the ACT has also explicitly recognised a right to 'privacy and reputation'. For example, the Victorian *Charter of Human Rights and Responsibilities Act 2006* states that:

> A person has the right—
>
> (a) not to have that person's privacy, family, home or correspondence unlawfully or arbitrarily interfered with; and
>
> (b) not to have that person's reputation unlawfully attacked.[38]

2.4.5 Several Australian inquiries and reports have recommended the introduction of similar human rights legislation in other Australian jurisdictions, including the Commonwealth and Tasmania. These include the Australian Human Rights Commission's 2022 Position Paper on a Human Rights Act for Australia and the TLRI's 2007 Final Report, A Charter of Rights for Tasmania. In the 2007 Final Report, the TLRI recommended that a Charter of Rights be enacted in Tasmania, which should protect

---

[34] Human Rights Committee, *CCPR General Comment No 16: Article 17 (Right to Privacy) The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation*, 32nd Sess (8 April 1988) [1] and [9] ('*General Comment No 16*').

[35] ICCPR art 17. See also *Universal Declaration of Human Rights*, GA Res 217A (III), UN GAOR, UN Doc A/810 (10 December 1948); *Convention on the Rights of the Child*, opened for signature 20 December 1989, 1577 UNTS 3 (entered into force 2 September 1990) art 16; *Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families*, opened for signature 18 December 1990, 2220 UNTS 3 (entered into force 1 July 2003) art 14.

[36] *General Comment No 16* [8].

[37] Human Rights Committee, *Views: Communication No 488/1992*, 50th Sess, UN Doc CCPR/C/50/D/488/1992 (31 March 1994) [8.3] ('*Toonen v Australia*'). This was a complaint brought before the United Nations Human Rights Committee against certain sections of the *Criminal Code* (Tas).

[38] *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13. The *Human Rights Act 2019* (Qld) s 25, and the *Human Rights Act 2004* (ACT) s 12, establish near-identical rights in Queensland and the ACT.

a comprehensive range of civil, political, economic, social, and cultural rights. The TLRI considered that a primary purpose of a Charter was to 'engender a human rights conscious culture within the Tasmanian community and across the three branches of government' (the legislature, the executive, and the judiciary).[39] This remains the view of the Tasmania Law Reform Institute.[40]

2.4.6 The Issues Paper to the present project invited submissions in response to the question:

> Should Tasmania codify a fundamental right to privacy, which can be set aside by other legislation that authorises activities that may interfere with privacy, and which is qualified by justified limitations?[41]

2.4.7 Four submitters offered brief responses to this question, with all of them supporting the legislative recognition of a right to privacy.[42] Two did not specify a view on the appropriate mechanism for this; the two others submitted that a right to privacy should be protected in a Human Rights Act or Charter, such as that proposed in the TLRI's 2007 Final Report. Meg Webb MLC submitted that this would 'provide a coherent and comprehensive framework in which our privacy statutes are derived and embedded'; the Tasmanian Council of Social Service ('TasCOSS') suggested that legislation in other jurisdictions provides an example of a charter containing a statutory right to privacy.

2.4.8 This Report does not seek to replicate or re-examine the case for human rights legislation which includes a right to privacy. As noted, the TLRI remains of the view that a human rights enactment should be introduced in Tasmania, which should include a right to privacy. The TLRI considers that protections created by such legislation would complement the protections of privacy that already exist in Tasmania, and the enhanced protections proposed in the Report.

2.4.9 The TLRI considers that a broad right to privacy would best be established in Tasmanian human rights legislation, rather than in privacy-specific Tasmanian legislation, such as the PIPA (discussed in Part 2 of this Report).[43] This is because, as noted at [2.5.1] below, neither the PIPA nor any other Tasmanian legislation provides broad privacy protection. Rather, Tasmanian legislation deals with a specific type of privacy (such as information privacy in the PIPA) or with privacy in a specific circumstance (such as protections against surveillance in the *Listening Devices Act 1991* (Tas) and the *Police Offences Act 1935* (Tas), respectively).

2.4.10 Other Parts of this Report include recommendations for reforms that would have a bearing on Tasmanians' rights in a more confined sense. These include proposals for the introduction of a right to erasure of personal information (also known as 'the right to be forgotten') and a right to object to the collection, use, or disclosure of personal information (see Part 5). This Report also assesses (in Part 11) the appropriateness of creating a statutory tort for serious invasions of privacy, which, the ALRC has suggested, would 'carr[y] the provisions of art 17(2) [of the ICCPR] into effect'.[44]

---

[39] Tasmania Law Reform Institute ('TLRI'), *A Charter of Human Rights for Tasmania* (Report No 10, October 2007) ('TLRI Final Report 2007') 3.
[40] TLRI, *A Charter of Rights for Tasmania? Update* (Research Paper No 6, April 2024).
[41] TLRI, *Review of Privacy Laws in Tasmania* (Issues Paper No 32, March 2023) Part 4, Question 4.8 ('Issues Paper').
[42] Submission 3 (Anonymous); Submission 20 (Dr Joel Scanlan); Submission 8 (Meg Webb MLC); Submission 11 (TasCOSS).
[43] The TLRI notes that this is consistent with the approach taken in the *Privacy Act Review Report* (Commonwealth of Australia, 2022) 21–22 <https://www.ag.gov.au/sites/default/files/2023-02/privacy-act-review-report_0.pdf> ('Privacy Act Review Report 2022'). The purpose and outcomes of that Review are introduced at [2.5.10] below.
[44] ALRC, *Serious Invasions of Privacy in the Digital Era* (Report 123) 64.

2.5 Existing privacy protections in Tasmania

2.5.1 There is no comprehensive privacy legislation in, or applying to, Tasmania. Rather, different (although sometimes overlapping) categories of privacy are protected under various laws that apply in a range of contexts.

2.5.2 These include:

- the Commonwealth *Privacy Act 1988* (Cth) ('Privacy Act'), which applies to the handling of personal information by Commonwealth government agencies and some private sector organisations around the country;
- Tasmania's *Personal Information Protection Act 2004* (Tas) ('PIPA'), which applies to information handling by Tasmanian government agencies; and
- a range of other statutes that provide some protections relating to information privacy, bodily privacy, territorial privacy, and/or communication privacy.

2.5.3 Tasmanian courts have also considered privacy protections in particular contexts.

2.5.4 This section briefly describes each of these existing privacy protections and explains where they are addressed in the substantive Parts of this Final Report.

The Privacy Act

2.5.5 The *Privacy Act 1988* (Cth) ('Privacy Act') is the primary piece of privacy legislation operating at the federal level in Australia. The Act was intended to partially implement Australia's privacy obligations under the ICCPR (described above at [2.4.1] and following).[45]

2.5.6 The Privacy Act, which enacted recommendations of a 1983 ALRC inquiry,[46] introduced 11 privacy principles applicable to the handling of personal information by Commonwealth government agencies and established a Privacy Commissioner to investigate complaints against mishandling.[47] In 2000, the Act was amended to establish a separate set of principles applicable to some private sector organisations.[48]

2.5.7 In 2012, following another ALRC inquiry,[49] the Privacy Act was further amended to provide a common set of privacy principles applicable to both the Commonwealth public sector and private organisations.[50] Known as the Australian Privacy Principles ('APPs'), they came into force on 12 March 2014.[51]

[45] *Privacy Act 1988* (Cth). In addition to partially implementing the ICCPR, the *Privacy Act 1988* (Cth) also implemented obligations under the Organization for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980): see Moira Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State* (Lexis Nexis, 2005) [2.54].
[46] Australian Law Reform Commission ('ALRC'), *Privacy*, ALRC 22 (1983).
[47] *Privacy Act 1988* (Cth), as at14 December 1988.
[48] *Privacy Amendment (Private Sector) Act 2000* (Cth), which commenced on 21 December 2001.
[49] ALRC, *For Your Information*.
[50] See Part 3.4 for a description of the public and private bodies bound by the *Privacy Act*.
[51] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth), which commenced on 12 March 2014.

2.5.8 The 13 APPs address:

1. Open and transparent management of personal information
2. Anonymity and pseudonymity
3. Collection of solicited personal information
4. Dealing with unsolicited personal information
5. Notification of the collection of personal information
6. Use or disclosure of personal information
7. Direct marketing
8. Cross-border disclosure of personal information
9. Adoption, use, or disclosure of government-related identifiers
10. Quality of personal information
11. Security of personal information
12. Access to personal information
13. Correction of personal information.[52]

2.5.9 The independent Office of the Australian Information Commissioner ('OAIC') was established to handle complaints under the Privacy Act (among other responsibilities).[53] The Information Commissioner must investigate complaints about acts or practices that may be an interference with privacy. If the Information Commissioner determines that a complaint is substantiated, they may make one or more declarations, including declarations that the conduct must not be repeated or continued, or that the complainant is entitled to compensation for loss or damage.[54]

2.5.10 As noted in [1.3.2] of this Report, the Commonwealth Attorney-General's Department commenced a review of the Privacy Act ('Privacy Act Review') in October 2020.[55] The review considered the scope and application of the Privacy Act and its protection of personal information, powers, and practices under that Act for monitoring and enforcement, and examined whether a Commonwealth statutory civil remedy for interference with privacy should be introduced. It also considered approaches to information privacy protection in overseas jurisdictions, including Canada and New Zealand, and the European Union's *General Data Protection Regulation 2016/679* ('GDPR').

2.5.11 The Privacy Act Review's Final Report was made public in February 2023. It contained 116 proposals for reform and reform-related activities to bring about major changes to how personal information is handled, how privacy protections are enforced, and how breaches of privacy are dealt with.

[52] *Privacy Act 1988* (Cth) sch 1.
[53] *Australian Information Commissioner Act 2010* (Cth).
[54] *Privacy Act 1988* (Cth) 52(1).
[55] Terms of Reference for the inquiry are available at <https://www.ag.gov.au/integrity/publications/review-privacy-act-1988-terms-reference>. An Issues Paper was published in October 2020 for consultation, which closed in November 2020. A discussion paper was released on 25 October 2021, with submissions due 10 January 2022. The report was released on 16 February 2023. See generally, Attorney-General's Department, 'Review of the Privacy Act 1988' (Web Page) <https://www.ag.gov.au/integrity/consultations/review-privacy-act-1988>.

2.5.12 The Commonwealth Government conducted a further round of consultations to inform its response to the Report, and published its response in September 2023. The Commonwealth Government agreed, or agreed in-principle, with the majority of the Privacy Act Review proposals. It undertook to develop legislative proposals and undertake further targeted consultation in relation to 'agreed' proposals, and to engage with entities (stakeholders) and conduct impact analysis to explore the implementation of proposals agreed to 'in-principle' in a manner that balanced privacy protections with impacts on regulated entities.[56]

2.5.13 Consideration of the adequacy of the Privacy Act in protecting Tasmanians' privacy was not within the scope of this project. This Report nevertheless discusses the Privacy Act provisions, and the Privacy Act Review, where doing so is necessary:

a) to identify, via comparative analysis, potential gaps in privacy protections in Tasmanian law and/or ways to address those gaps (consistent with the Terms of Reference set out at [1.2]); and/or

b) to assess whether gaps in Tasmanian privacy laws are already addressed at the Commonwealth level and hence do not require a state-level response.

The Personal Information Protection Act 2004 (Tas) ('PIPA')

2.5.14 Tasmania, as with all State and Territory jurisdictions except Western Australia and South Australia, has general legislation regulating how the state or territory public sector can handle personal information.[57] These laws generally establish privacy principles that constitute some variation on the Commonwealth APPs and establish a process for investigation of complaints by an independent body (see Appendix 1 for a description of privacy frameworks in other states and territories).

2.5.15 In Tasmania, the *Personal Information Protection Act 2004* (Tas) ('PIPA') is the primary law for the protection of information privacy regarding information held by Tasmanian government agencies. The PIPA was passed in 2004 with broad bi-partisan support.[58] Its key objective was to 'ensure that the way in which the State and local government sectors collect, use, and disclose personal information is fully transparent'.[59] The PIPA was a response to community concerns about the need to ensure 'government bodies respect and properly control the personal information they collect and hold'[60] in light of the growth of the information economy and increasing use of the internet to deliver government services. The introduction of the PIPA followed the expansion of Commonwealth privacy protection from the public sector to the private sector described at [2.5.7] above and was similar to legislation enacted in New South Wales, Victoria, and the Northern Territory.

2.5.16 The PIPA generally requires public authorities and their contractors to comply with 10 Personal Information Protection Principles ('PIPPs') when handling personal information, although there are multiple exceptions established in the PIPA and in other legislation. In summary, the PIPPs address:

---

[56] Australian Government, *Government Response: Privacy Act Review Report* (2023) 2 <https://www.ag.gov.au/sites/default/files/2023-09/government-response-privacy-act-review-report.PDF> ('Government Response').

[57] In South Australia—where there is no general privacy legislation—non-legislative administrative schemes address complaints about the handling of personal information by the public sector.

[58] See Tasmania, *Parliamentary Debates*, House of Assembly, 20 October 2004, pt 2, 62–4, 96–8.

[59] See the Second Reading speech for the *Personal Information Protection Bill 2004* (Tas): Tasmania, *Parliamentary Debates*, House of Assembly, 20 October 2004, 63.

[60] Ibid 62.

1. the collection of personal information;
2. the use and disclosure of personal information;
3. the quality of personal information;
4. safeguarding personal information from misuse, loss, unauthorised access, modification or disclosure;
5. openness regarding policies on the handling of personal information;
6. the ability of individuals to access and correct their personal information;
7. the assignment of unique identifiers to individuals;
8. allowance of anonymous dealings with agencies;
9. disclosure of personal information to a body outside of Tasmania; and
10. the collection of sensitive information, such as information on race, ethnicity, or criminal history.

2.5.17 Complaints relating to a contravention of the PIPPs can be made to the Ombudsman, who may either deal with the matter or refer it to another person, body, or authority. If the Ombudsman finds a contravention, the Ombudsman must provide this advice and any recommendations to the Minister for Justice and Industrial Relations;[61] the Minister must table the advice and recommendations in both Houses of Parliament within 5 sitting days.[62]

2.5.18 Parts 2–4 of this Report consider the adequacy of the PIPA in protecting Tasmanians' privacy. It identifies a range of gaps or shortcomings of the existing system and recommends a range of reforms.

Other Tasmanian legislation

2.5.19 Other legislation affects the Tasmanian Government's access to, and use or disclosure of, personal information. Some is general in scope, such as the *Right to Information Act 2009* (Tas), which creates a legally enforceable right for a person to be provided information held by a public authority or Minister.[63] Other legislation only applies in specific contexts. For example, provisions of the *Family Violence Act 2004* (Tas), the *Children, Young Person and their Families Act 1997* (Tas) and the *Dangerous Criminals and High Risk Offenders Act 2021* (Tas) (among others) qualify or exempt personal information custodians from the operation of the PIPA in specific circumstances.

2.5.20 Part 9 of this Report examines the adequacy of this other legislation that bears on privacy relating to government-held information.

2.5.21 Other legislative privacy protections extend beyond the protection of government-held information and information privacy rights. Information privacy rights relating to individuals' health information are also protected by provisions of the *Health Complaints Act 1995* (Tas) and the *Tasmanian Charter of Health Rights and Responsibilities*. Bodily and territorial privacy, otherwise known as rights to seclusion, are also protected through legislation including:

[61] To whom responsibility for administration of the PIPA is assigned: *Personal Information Protection Act 2004* (Tas) s 24 ('PIPA').
[62] PIPA s 22.
[63] *Right to Information Act 2009* (Tas) s 7 ('RTI Act').

- the *Listening Devices Act 1991* (Tas), which restricts the use of listening devices to record and listen to private conversations;
- criminal laws, such as the *Police Offences Act 1935* (Tas), which makes it an offence to observe or visually record another person in breach of privacy, and the *Criminal Code* (Tas), which makes it a crime to engage in stalking or bullying;
- the *Evidence Act 2001* (Tas), which states that inconsistency with a right recognised in the ICCPR is one matter that a court may take into consideration in determining whether evidence improperly or illegally obtained should be admitted;[64]
- legislation where the powers or activities regulated by the legislation may impact on a person's privacy, such as the *Children, Young Persons and Their Families Act 1997* (Tas)[65] and the *Disability Services Act 2011* (Tas),[66] which correspondingly mandate that children and persons with disability must be treated in a manner respecting their dignity and privacy; and
- legislation that affords specific privacy protections in particular circumstances, such as the *Residential Tenancy Act 1997* (Tas), which states that all non-social housing residential tenancy arrangements must include window coverings for privacy,[67] and the *Access to Neighbouring Land Act 1992* (Tas), which holds that, if a court has granted an order permitting a person to access to neighbouring land to carry out work (such as to repair drains), the order may be subject to conditions to avoid or minimise loss of privacy.[68]

2.5.22 Part 10 of this Report discusses the adequacy of other Tasmanian laws in protecting individuals' information, bodily, and territorial privacy.

The general law in Tasmania

2.5.23 Tasmanian courts have acknowledged privacy, or a right to privacy, as a relevant consideration in a small number of cases. These cases have generally involved the interpretation and application of legislation that obliges decision-makers to treat privacy as a relevant consideration, or to consider Australia's obligations under the ICCPR more generally. For example, in several cases concerning whether improperly or illegally obtained evidence should be admitted under the *Evidence Act 2001* (Tas) (see [2.5.21] above), the Tasmanian Supreme Court has determined that one factor weighing against the evidence being admitted is that the evidence was obtained in a manner that constituted an interference with the accused's right to privacy under art 17 of the ICCPR.[69]

2.5.24 In the 2019 case of *Clubb v Edwards; Preston v Avery*, the majority of the High Court of Australia also inferred a legislative purpose to 'protect the safety, wellbeing, privacy and dignity of

[64] *Evidence Act 2001* (Tas) s 138(3)(f). The Tasmanian Supreme Court has in several cases identified contraventions of the art 17 right to privacy as a relevant matter in determining the admissibility of evidence: *R v Brown* [2014] TASSC 18; *R v Pettit* [2015] TASSC 14; *Tasmania v Wykes* [2019] TASSC 18.
[65] *Children, Young Persons and Their Families Act 1997* (Tas) s 10D(1).
[66] *Disability Services Act 2011* (Tas) s 5(1)(j). The *Disability Inclusion Bill 2023* (Tas) replicates this principle in cl 8(1)(l).
[67] *Residential Tenancy Act 1997* (Tas) s 36N(1). The *Residential Tenancy Amendment (Minimum Window Coverings for Social Housing Properties) Act 2023* (Tas), which comes into force in mid-2024, will amend the *Residential Tenancy Act* to extend the requirement for minimum window coverings to be provided in social housing residential properties.
[68] *Access to Neighbouring Land Act 1992* (Tas) s 6(2)(b).
[69] *R v Brown* [2014] TASSC 18; *R v Pettit* [2015] TASSC 14; *Tasmania v Wykes* [2019] TASSC 18; see also *Hibble v B* [2012] TASSC 59. Cf *Tasmania v Melick* [2019] TASSC 19, where the Court held the evidence to be admissible in spite of the privacy interference, because the interests in privacy were outweighed by countervailing public interests in crime detection.

persons accessing' abortion clinics[70] in the *Reproductive Health (Access to Terminations) Act 2013* (Tas) and considered this to be a 'legitimate purpose' that—in combination with other factors — constituted a justifiable interference with the implied constitutional right to freedom of political communication of anti-abortion protestors.[71]

2.5.25 Neither Commonwealth nor state and territory (including Tasmanian) courts have recognised a standalone right to privacy, nor a legal avenue for people to seek compensation for serious invasions of their privacy in most areas of life. For example, the High Court of Australia raised the possibility of the establishment of a standalone action for interference with privacy in the 2001 case of *Lenah Game Meats*,[72] but the common law has not developed since that time. Consequently, there is no avenue for Tasmanians—or for people in other Australian jurisdictions—to seek compensation for violations of bodily privacy or territorial privacy, or for violations of information privacy by individuals or other entities not covered by legislation.[73]

2.5.26 Part 11 of this Report discusses general law privacy protections and recommends the enactment of a statutory tort for serious invasions of privacy either in Tasmania or at the Commonwealth level.

2.6 Consistency of information privacy regulation across jurisdictions

2.6.1 A key issue identified in reviews elsewhere in Australia, and in submissions to the present project, is the desirability of consistency between Tasmanian privacy legislation and legislation in other jurisdictions, especially in regard to the regulation of information privacy.

2.6.2 Consecutive Australian inquiries have argued in favour of consistency of privacy laws around the country to minimise cost and confusion. For example, the ALRC argued in its 2008 privacy report that:

> Inconsistency and fragmentation in privacy regulation causes a number of problems, including unjustified compliance burden and cost, impediments to information sharing and national initiatives, and confusion about who to approach to make a privacy complaint. National consistency, therefore, should be one of the goals of privacy regulation.[74]

2.6.3 The ALRC recommended that consistency could best be achieved if the Commonwealth legislates exclusively with respect to the handling of personal information by non-government organisations, subject to some matters reserved to states and territories, including matters regarding public health.[75] It encouraged state and territory governments to promote and maintain uniformity by agreeing to implement legislation for a set of common privacy principles applicable to government agencies.[76]

[70] *Clubb v Edwards; Preston v Avery* (2019) 267 CLR 171 [120].
[71] (2019) 267 CLR 171 [120].
[72] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 ('*Lenah Game Meats*').
[73] Privacy Act Review Report 2022 280ff.
[74] ALRC, *For Your Information* [3.13].
[75] Ibid 218–12, Recommendations 3-1, 3-2, 3-3.
[76] Ibid 219–20, 224, Recommendations 3-4, 3-5.

2.6.4 More recently, the Privacy Act Review proposed in its 2022 Final Report that a Commonwealth, state, and territory working group be established to harmonise legislation, especially in relation to 'areas of key concern', such as the treatment of health information, the treatment of contractors[77] and the scope of research exceptions.[78] The Commonwealth Government agreed in-principle with this proposal.[79]

2.6.5 Consistency has been considered an important law reform goal in reviews of privacy legislation in other state and territory jurisdictions. For example:

- In New South Wales ('NSW'), a 2010 review of privacy protection recommended the adoption of uniform privacy principles across Australia. The review recommended that national model privacy principles apply to private organisations as third-party contractors, and the NSW legislation be amended to apply the principles to public sector bodies.[80]
- In Western Australia, a 2019 discussion paper proposed using the APPs as the basis for establishing regulation for the collection and use of personal information.[81]
- In 2020, the Queensland Crime and Corruption Commission recommended that the *Information Privacy Act 2009* (Qld) be updated to reflect a common set of privacy principles based on the APPs.[82]

2.7 Consultation

2.7.1 The Issues Paper for this project invited submissions on the following question:

> Should the PIPPs under the Tasmanian PIPA be amended to make them, as far as possible, consistent with the APPs in the Commonwealth Privacy Act as they currently exist or as amended in the future?[83]

2.7.2 Several submissions were supportive of greater consistency. The Tasmanian Ombudsman stated that consistency between schemes across the states and the Commonwealth, including providing similar protections and remedies, 'makes sense'.[84] Other submissions argued that consistency would offer greater clarity and certainty, both to individuals and regulated entities. For example, Youth Law Australia argued that the complexity and fragmentation of privacy law 'makes it difficult for

[77] Privacy Act Review Report 2022 Proposal 29.3, 302–303.
[78] Ibid Proposal 29.3, 138.
[79] Australian Government, *Government Response: Privacy Act Review Report* (2023) 16.
[80] NSW Law Reform Commission, *Privacy Principles* (Report No 123, August 2009) 4, 198–9 (see Recommendation 11); NSW Law Reform Commission, *Protecting Privacy in New South Wales* (Report No 127, May 2010) 35–6 (see Recommendation 2.5).
[81] Government of Western Australia, *Privacy and Responsible Information Sharing for the Western Australian Public Sector* (Discussion Paper, 2019).
[82] Crime and Corruption Commission (Queensland), *Operation Impala: Report on Misuse of Confidential Information in the Queensland Public Sector* (Report, February 2020) Recommendation 16. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) has been passed but not commenced, which would amend the Queensland Privacy Principles to reflect the Commonwealth APP (now called Queensland Privacy Principles ('QPP') rather than schedule 3 (IPPs) and schedule 4 (PP). This Act implements or responds to reforms proposed in a number of Queensland reviews of information privacy and right to privacy: see *Information Privacy and Other Legislation Amendment Act 2023* (Qld) Explanatory Notes <https://documents.parliament.qld.gov.au/bills/2023/3163/Information-Privacy-and-Other-Legislation-Amendment-Bill-2023---Explanatory-Notes-baf8.pdf>. The full details of the background to the reforms and the legislative changes are beyond the scope of this report.
[83] Issues Paper Part 2, Question 2.7.
[84] Submission 4 (Tasmanian Ombudsman).

organisations to understand their obligations, and for children and young people (among others) to understand their rights and access remedies'.[85]

2.7.3 The Insurance Council of Australia cautioned against unnecessary duplication of Commonwealth laws and regulations in state and territory reforms.[86] It also observed that the Commonwealth Privacy Act Review was still ongoing because the Review's Final Report recommended further consultation on several of its proposals and it is currently unclear which of the Review's proposals will be implemented by the Commonwealth Government.[87] The TLRI notes that the Commonwealth Government has since published its response to the Review's proposals (see [2.5.12] above) but the precise wording of legislative reforms is still to be developed.

2.7.4 Several submissions also noted the importance of consistency, not only within Australia, but between Australian and international privacy protection standards.[88] The Privacy Act Review similarly discussed consistency with international regimes at several points in its Final Report. It noted, for example, that multiple submitters supported reforms to the data breach notification scheme that would be consistent with international jurisdictions, although others expressed concern that 'the pursuit of harmonisation' might result in greater regulatory burden, or argued for single reporting agencies and mechanisms rather than dual reporting.[89] This is discussed further at [8.12]–[8.15].

2.8 The TLRI's view

2.8.1 In the TLRI's view, consistency of the Tasmanian information privacy legislation with the Commonwealth and other state and territory legislation is desirable for reasons including: reducing confusion; enabling information sharing; and enabling Tasmania to learn from the experiences and review and inquiry processes undertaken in those other jurisdictions.

2.8.2 The TLRI agrees with the Privacy Act Review that a Commonwealth, State, and Territory working group should be established to discuss aligning privacy legislation and working towards a model for harmonisation.[90] The advantages of consistency across jurisdictions, and the implications of this for particular elements of the PIPA, are discussed in more detail in Parts 3, 4 and 5 of this Final Report.

[85] Submission 12 (Youth Law Australia) 3.
[86] Submission 7 (Insurance Council of Australia).
[87] Ibid.
[88] Submission 7 (Insurance Council of Australia); Submission 20 (Dr Joel Scanlan).
[89] Privacy Act Review Report 2022 290, 291 and citing several submissions.
[90] Privacy Act Review Report 2022 Proposal 29.3 303.

Part 3

Scope and Application of the *Personal Information Protection Act 2004* (Tas) ('PIPA') – Bodies Subject to the PIPA

3.1 Overview of this Part

3.1.1 The Terms of Reference ('ToRs') and the Issues Paper raised a series of questions about the adequacy of the PIPA under three broad themes, which this Part addresses in turn:

- whether there should be amendments to the scope and application of the PIPA (Parts 3 and 4);
- whether there should be amendments to the PIPPs (Parts 5—7); and
- whether there should be amendments to complaints, monitoring, and enforcement mechanisms (Part 8).

3.1.2 This Part examines the scope and application of the PIPA and considers whether the PIPA, which applies broadly to Tasmanian public authorities and some government contractors, should apply to other bodies.

3.2 The Tasmanian position

3.2.1 The PIPA broadly applies to state public authorities and some government contractors. These bodies are referred to as 'personal information custodians'.[91] The PIPA adopts the meaning of 'public authority' in Section 6 of the *Right to Information Act 2009* (Tas), which holds that a public authority is:

- an Agency (comprising government departments and state authorities);[92]
- the University of Tasmania;
- the Police Service;
- a council;
- a statutory authority;
- a body (corporate or unincorporate) established under legislation for a public purpose;
- a body whose members (or a majority of members) are appointed by the Governor or a Minister of the Crown;

[91] Note that public information custodians can also be prescribed in regulations, but at present there are no regulations for the PIPA.
[92] The meaning of 'Agency' is adopted from that in the *State Service Act 2000* (Tas), which lists all agencies in Schedule 1: *State Service Act 2000* (Tas) s 3(1) ('Agency').

- a Government Business Enterprise;[93]
- a Council-owned company; or
- a State-owned company.[94]

3.2.2 Certain public bodies are exempt from the provisions of the PIPA, either generally or when exercising their official functions. Courts and tribunals and registries or other offices of such courts and tribunals are exempt in relation to the performance or exercise of judicial or quasi-judicial functions or powers, while holders of a judicial or quasi-judicial office pertaining to a court or tribunal are exempt in the capacity of the holder of that office.[95] Other exempt bodies include the Solicitor-General and employees, the Director of Public Prosecutions and employees, and the Integrity Commission.[96]

3.2.3 The PIPA creates another exemption in relation to disclosure of personal information for the purpose of obtaining legal advice. Such disclosure is permitted to the Solicitor-General, Director of Public Prosecutions or Crown Solicitor, or to people employed in relation to those offices' functions or duties.[97]

3.2.4 The PIPA only applies to private or non-government bodies in a limited range of circumstances; namely, where such a body has entered a contract with a public authority and the contract involves the collection, use, or storage of personal information.[98] In these circumstances, such bodies are deemed 'personal information custodians' and must comply with the Personal Information Protection Principles ('PIPPs'). The PIPPs consequently apply to all that body's dealings with personal information—not only those dealings that relate to personal information collected, used, or stored under the contract in question.

3.2.5 Examples of circumstances in which a contracted body will be bound by the PIPPs include:

- where a public authority has outsourced some aspect of personal information management to a private organisation that provides cloud computing services;[99] and
- where a public authority has contracted a non-government organisation to provide a service to the public and delivery of the service involves the collection, use, or storage of personal information.

3.2.6 Private bodies may also be bound by legislative privacy protections if they are a health service provider. Health services that are provided by personal information custodians are bound by the PIPA (discussed below in [Parts 5–8]), while public and private health service providers have some privacy-related obligations under the *Tasmanian Charter of Health Rights and Responsibilities* and the *Health Complaints Act 1995* (Tas) (discussed at [10.17]).

[93] The meaning of 'Government Business Enterprise' is adopted from the *Government Business Enterprises Act 1995* (Tas), which specifies a list of statutory authorities that constitute a Government Business Enterprise at Schedule 1: *Government Business Enterprises Act 1995* (Tas). They are: Forestry Corporation established by the Forestry Act 1920; Hydro-Electric Corporation; Motor Accidents Insurance Board; Port Arthur Historic Site Management Authority; Public Trustee; and Tasmanian Public Finance Corporation: ibid, Sch 1.
[94] PIPA s 3 ('public authority'); see *Right to Information Act 2009* (Tas) s 5.
[95] PIPA s 7(a), (b), (g).
[96] PIPA s 7(c), (d), (e), (f), (ga), (h).
[97] PIPA s 12A.
[98] PIPA s 3 (definition of 'personal information custodian' and 'personal information contract'); s 17.
[99] Note that use of cloud storage may come within the terms of s 12 of the PIPA, which provides for the efficient storage and use of basic information. See further the discussion of 'basic personal information' in Part 4].

Obligations under Commonwealth privacy laws for Tasmanian bodies

3.2.7 Tasmanian bodies may also be subject to information privacy obligations under the Commonwealth *Privacy Act 1988* (Cth) ('Privacy Act'). While the intention of the federal law is not to affect state or territory laws that regulate personal information in a way that can operate concurrently with the federal law,[100] there are some areas of potential overlap.

3.2.8 The Australian Privacy Principles ('APPs') apply to 'APP entities'; namely, agencies and organisations as defined in the Privacy Act.[101]

- 'Agencies' include Ministers, Departments, bodies, tribunals and offices made under Commonwealth law (or under State and Territory law where in force in an external Territory), appointees of the Governor-General, federal courts, the Australian Federal Police and others;[102]
- 'Organisations' comprise individuals, corporations, partnerships, unincorporated associations, and trusts, where they provide a health service, deal with personal information on a commercial basis, are contractors with the Commonwealth government to provide services to the public, or have an annual turnover of more than $3 million.[103]

3.2.9 Some bodies that would meet the Privacy Act definition of an organisation are exempt from the operation of the Privacy Act. These include:

- a general exemption from the application of the Act to small business operators (operators of a small business with an annual turnover of $3 million or less);[104]
- a general exemption from the application of the Act for political parties registered under the *Commonwealth Electoral Act 1918* (Cth);[105] and
- exemption of political representatives and their affiliates (contractors and sub-contractors), and affiliates of registered political parties (contractors, sub-contractors, and volunteers) from the Act in a narrower set of circumstances in connection with elections, a referendum, or participation in another aspect of the political process.[106]

3.2.10 Small businesses that trade in personal information—that is, disclose personal information for a benefit, service, or advantage—are outside the scope of this exemption,[107] unless they obtain the consent of individuals to collect or disclose their personal information.[108]

3.2.11 State or Territory public authorities are also generally exempt from the operation of the Privacy Act.[109] Contractors engaged by State public authorities to provide services are also exempted

[100] *Privacy Act 1988* (Cth) s 3.
[101] *Privacy Act 1988* (Cth) s 6 (definition of 'APP entity' and 'organisation').
[102] See *Privacy Act 1988* (Cth) s 6 (definition of 'agency').
[103] See *Privacy Act 1988* (Cth) ss 6 (definition 'organisation'), 6D.
[104] *Privacy Act 1988 (Cth)* ss 6C(1), 6D. Small businesses that trade in personal information (that is, disclose personal information for a benefit, service or advantage) are outside the scope of this exemption, unless they obtain the consent of individuals to collect or disclose their personal information: *Privacy Act 1988* (Cth) ss 6D(4)(c), (7).
[105] *Privacy Act 1988* (Cth) ss 6 (definition of 'registered political party'), 6C(1).
[106] *Privacy Act 1988* (Cth) ss 6C, 7C; Review Report 2022 72.
[107] *Privacy Act 1988* (Cth) s 6D(4)(c).
[108] *Privacy Act 1988* (Cth) ss 6D(7).
[109] *Privacy Act 1988* (Cth) ss 6C(1), (3). This includes bodies or tribunals established or appointed for a public purpose under a State or Territory law, except where that body is an incorporated company, society, or association. Note that States and Territories can also request that their instrumentalities be exempted.

from the Privacy Act, but only in relation to acts or practices for the purposes of meeting obligations under the contract.[110]

3.2.12 Organisations may be subject to both the Commonwealth Privacy Act and the Tasmanian PIPA. For example, a private body might have an annual turnover of greater than $3 million and hence be subject to the Commonwealth APPs, while also being party to a personal information contract with the Tasmanian Government and hence subject to the Tasmanian PIPPs (and not the APPs) in relation to that contract.

3.3 The position in other jurisdictions

3.3.1 As noted in Part 2, information privacy legislation exists in all other State and Territory jurisdictions except Western Australia and South Australia. Statutes in these other jurisdictions have similarly broad application to State or Territory public authorities, with courts and tribunals being treated differently such that they are not bound in their judicial functions but are bound in their administrative functions.[111] Royal Commissions and Commissions of Inquiry are also typically exempted.[112]

3.3.2 The legislation in other jurisdictions generally limits the extent to which protections apply beyond the public sector in similar ways to the PIPA.[113] As in Tasmania, private bodies in these other jurisdictions that must typically comply with the legislative obligations are government contractors and private health service providers.[114] The latter must comply with both Commonwealth and State/Territory privacy laws when handling health information.[115]

3.3.3 Unlike in Tasmania, where protections apply automatically when a contractor enters an outsourcing arrangement with a government agency, Victorian and Queensland agencies must take positive steps to bind a contractor to the state privacy principles.[116] Further:

[110] *Privacy Act 1988* (Cth) ss 6 (definition of 'State contract'), 7B(5).
[111] For example, *Privacy and Personal Information Protection Act 1998* (NSW) s 6(1); *Privacy and Data Protection Act 2014* (Vic) s 10; *Information Privacy Act 2009* (Qld) s 19; Sch 2, Pt 2; *Information Privacy Act 2014* (ACT) s 25(1)(b). It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) has been passed but not commenced. Details of the reforms are outlined in *Information Privacy and Other Legislation Amendment Act 2023* (Qld) Explanatory Notes <https://documents.parliament.qld.gov.au/bills/2023/3163/Information-Privacy-and-Other-Legislation-Amendment-Bill-2023---Explanatory-Notes-baf8.pdf>.
[112] For example, *Privacy and Data Protection Act 2014* (Vic) ss 10A, 11; *Privacy and Personal Information Protection Act 1998* (NSW) s 6(2); *Information Privacy Act 2009* (Qld) s 19; Sch 2, Pt 1. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) has been passed but not commenced. *Information Privacy and Other Legislation Amendment Act 2023* (Qld) Explanatory Notes.
[113] For example, *Privacy and Personal Information Protection Act 1998* (NSW) s 3 (definition of 'public sector agencies'), s 20; *Privacy and Data Protection Act 2014* (Vic) s 13; *Information Privacy Act 2009* (Qld) ss 18, 21; *Information Privacy Act 2014* (ACT) s 9; *Information Act 2002* (NT) s 5. See *Information Privacy and Other Legislation Amendment Act 2023* (Qld) Explanatory Notes, for discussion of reforms contained in the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) (yet to commence).
[114] For example, *Privacy and Data Protection Act 2014* (Vic) s 13.
[115] *Health Records (Privacy and Access) Act 1997* (ACT) Dictionary (definition of 'health service' and 'health service provider'); *Health Records and Information Privacy Act 1998* (NSW) s 4 (definition of 'health service' and 'health service provider'; *Health Records Act 2001* (Vic) s 3 (definition of 'health service provider') s 11.
[116] *Privacy and Data Protection Act 2014* (Vic) ss 13(1)(j), 17(2); *Information Privacy Act 2009* (Qld) ss 34–7.

- In Victoria, a government contractor is bound only where the contract contains a term providing for this restriction.[117] This contractual term also affects who is held responsible for interferences with privacy. Unless the term was both included in the contract and capable of being enforced against the contractor, any interference with privacy is taken to be engaged in by both the government agency and the contractor.[118]
- In Queensland, a government contractor is bound only where the government agency has taken all reasonable steps to ensure this.[119] If such reasonable steps have not been taken, the government agency remains responsible for breaches of privacy.

3.4 The Commonwealth Privacy Act Review

3.4.1 The Privacy Act Review considered the appropriateness of the Privacy Act exemptions for private bodies (small businesses) and political parties, representatives, and affiliates (discussed at [3.2.9] above). These proposals concerned matters that are not dealt with in Tasmanian legislation, but may have impacts on Tasmanian businesses and political entities.

3.4.2 The Review examined whether small business exemptions which limit the Privacy Act's application to the private sector should be removed or amended.[120] In its Final Report, the Review proposed that the small business exemption be removed on the basis that the growing use of digital technology by businesses was creating greater privacy risks and the application of privacy protections in relation to small businesses' handling of personal information would benefit individuals.[121]

3.4.3 The Review recommended that the exemption only be removed after several steps are taken, including: analysing the impacts of such reform on small business; developing support for small business; and identifying (in consultation with small business) of the most appropriate way for small business to meet obligations proportionate to risk is determined (in consultation with small business).[122] In its response, the Commonwealth Government agreed in-principle with these reforms and undertook to consult further to understand the potential impacts of such reforms on small businesses and identify appropriate privacy protections and supports.[123]

3.4.4 The Review proposed that, in the shorter term, the small business exemption be removed in relation to the collection of biometric information for use in facial recognition technology (discussed in detail at [3.6.2]) and in relation to small businesses that trade in personal information, which is presently permitted where individuals' consent is obtained (see [3.2.10]).[124] These proposals reflect the high privacy risks associated with these activities.[125] The Commonwealth Government also agreed in-principle with this proposal.

3.4.5 The Review also considered the Privacy Act exemptions relating to registered political parties, political representatives and their affiliates, and affiliates of registered political parties.[126] The Final

[117] *Privacy and Data Protection Act 2014* (Vic) ss 13(1)(j), 17(2).
[118] Ibid s 17(4).
[119] *Information Privacy Act 2009* (Qld) ss 34–7. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) has been passed but not commenced.
[120] Privacy Act Review Report 2022 28.
[121] Ibid ch 6.
[122] Ibid Proposal 6.1.
[123] Government Response 6.
[124] Privacy Act Review Report 2022 Proposal 6.2.
[125] Ibid 61.
[126] *Privacy Act 1988* (Cth) ss 6C, 7C; Review Act Review Report 2022 72

Report stated that the political exemption 'was introduced to encourage freedom of political communication and enhance the operation of the electoral and political process',[127] and observed that technological advances mean greater volumes of data about voters can be collected and utilised for political influence, raising concerns about privacy and the adequacy of the exemption. According to the Review, most of the submissions that addressed this exemption expressed the view that the exemption was not justifiable and should be narrowed or removed.[128]

3.4.6 The Review proposed that the political parties exemption be narrowed to match the exemption currently available to political representatives and affiliates (described at [3.2.9] above), meaning they would be subject to the APPs except where handling information for purposes connected to the political process.[129] The Review asserted that this would be more closely aligned with the purpose of the exemption.[130] It also proposed that political entities covered by the political exemption should be required under the Privacy Act to have a privacy policy, on the basis that this would provide greater transparency.[131] Privacy policies are discussed further in [7.2] of this Report.

3.4.7 The Review further proposed a range of new qualifications or limitations on the political exemption. These included:

- introducing a 'fair and reasonable' test to determine when the exemption applies to political acts and practices (discussed further in [3.6.3] of this Report);
- prohibiting political entities from engaging in targeting based on sensitive information or traits relating to an individual (with some exceptions in relation to political opinions and membership of a political association or trade union);[132]
- requiring entities to give individuals the means to opt-out of their personal information being used or disclosed for direct marketing or targeted advertising;[133]
- requiring political entities to take reasonable steps to protect the personal information and destroy or de-identify it once it is no longer needed for the purpose covered by the exemption;[134] and
- requiring political entities to comply with the notifiable data breaches scheme (discussed at [8.12] of this Report).[135]

3.4.8 In its response to the Privacy Act Review Final Report, the Commonwealth Government noted the Review's proposals regarding narrowing the political exemption and did not indicate an intention to pursue reforms in this regard.

3.4.9 The Privacy Act Review also acknowledged multiple areas of complexity in the interaction of Commonwealth and State and Territory legislation, several of which related to the types of entities subject to Commonwealth and/or State and Territory legislation. It recommended the establishment of

[127] Review Act Review Report 2022 72.
[128] Privacy Act Review Report 2022 73.
[129] Ibid Proposal 8.1.
[130] Ibid 74.
[131] Ibid Proposal 8.2.
[132] Ibid Proposal 8.3. The Review echoed the Australian Law Reform Commission's recommendation of the inclusion of a 'savings clause' to allow courts to read down the Act to ensure its constitutional validity in terms of interference with implied freedom of political communication: Proposal 8.2.
[133] Ibid Proposal 8.4.
[134] Ibid Proposal 8.5.
[135] Ibid.

a Commonwealth, State, and Territory working group to 'provide a forum to focus on aligning privacy legislation in areas of key concern', including:

- pursuing the harmonisation of health privacy legislation in light of its complexity and a need for clarification in relation to issues, such as the growth of telehealth services and the treatment of genomic information and coverage of deceased persons;[136] and
- addressing concerns about gaps in coverage of privacy protections where contractors under State or Territory contracts are exempt from the APPs to the extent of that contract, regardless of whether State or Territory legislation applies to acts and practices performed under the contract; as discussed at [3.2.4] above, the PIPA does apply in these circumstances in Tasmania.[137]

3.5 Consultation

3.5.1 In the Issues Paper, the following questions were posed about the scope of bodies subject to the PIPA:

> Are there Tasmanian public sector agencies or organisations not sufficiently covered by the PIPA, or which should otherwise be included in the definition of 'personal information custodian'?[138]
>
> Should non-government organisations, such as for-profit businesses, charities, or political parties registered in Tasmania, be subject to privacy regulation in addition to any obligations under the Privacy Act?[139]
>
> To what extent are government contractors appropriately subject to obligations under the PIPA? Should there be additional obligations on Tasmanian government agencies entering into contracts with private bodies to ensure that privacy obligations are able to be enforced against the contractor?[140]

3.5.2 A small number of submissions to this project expressed views in response to these questions. In relation to Question 2.1, Meg Webb MLC submitted that all public sector agencies, including those currently exempt, should be subject to the PIPA and defined as 'personal information custodians'.[141] Ms Webb proposed that the PIPA could provide access to exemptions for courts and tribunals and other public legal officers and employees 'when supported by a public interest test'.[142]

3.5.3 In response to Question 2.2, several submitters expressed the view that non-government organisations should be subject to the same privacy regulation as other entities where they are in a position to obtain basic information or sensitive information, although none expressed a view about whether this necessitated amendment of the PIPA or was more appropriately dealt with elsewhere, such as in the Commonwealth Privacy Act.[143]

[136] Privacy Act Review Report 2022 302.
[137] Ibid Proposal 29.3 303.
[138] Issues Paper Part 2, Question 2.1.
[139] Ibid Part 2, Question 2.2.
[140] Issues Paper Part 2, Question 2.3.
[141] Submission 8 (Meg Webb MLC).
[142] Ibid.
[143] Submission 3 (Anonymous); Submission 8 (Meg Webb MLC).

3.5.4 Tasmania Legal Aid ('TLA') suggested that 'questions around the inability to "guarantee" regulated information-handling in NGOs' were inhibiting information sharing by government bodies in circumstances where government and non-government organisations have mutual clients but not contractual arrangements. TLA called for facilitation of information sharing between organisations, including government organisations and NGOs.[144] Information sharing between government bodies is discussed in detail at [9.10]–[9.13] of this Report.

3.5.5 In response to Question 2.3, Meg Webb MLC submitted that government contractors 'can be a potential "loop-hole" in [the] context of consistent and rigorous application of privacy protections'. Ms Webb called for 'clear and reportable additional obligations on Tasmanian government agencies entering into contracts with private bodies' to ensure privacy obligations can be enforced against those contractors.[145]

3.6 The TLRI's view

3.6.1 The TLRI is of the view that there is not a strong argument for the extension of the scope of the PIPA to apply to additional Tasmanian public sector agencies or organisations, such as courts and tribunals. The TLRI notes that such reforms would be inconsistent with the scope of legislation in other state jurisdictions with information privacy legislation, such as New South Wales, Victoria, and Queensland, and also the position under the *Privacy Act 1988* (Cth). An amendment to remove the exemption for courts and tribunals acting in a judicial capacity would be contrary to longstanding principles of open justice.[146]

3.6.2 Similarly, the TLRI is of the view that there is not a clear argument for extending the scope of the PIPA to apply to non-government organisations. The TLRI's view is that this is, instead, a matter more appropriately addressed under the Commonwealth Privacy Act framework. As observed in the Issues Paper, the imposition of broad obligations on private organisations, in the absence of a sufficient connection to the Tasmanian public sector, would generally be restricted by the fact that the Commonwealth Privacy Act already applies to those organisations. As discussed at [3.4.4] and following above, the Privacy Act Review and the Commonwealth Government's in-principle agreement suggests that the small business exemption may be removed in relation to the collection of biometric information for use in facial recognition technology and small businesses trading in personal information in the shorter term. Further, the TLRI notes the Commonwealth's in-principle agreement with the broader proposal to remove the small business exemption from the Privacy Act, the adoption of which would extend privacy protections in relation to these bodies' handling of personal information.

3.6.3 The TLRI notes that the Commonwealth Government has not expressed an intention to alter the political party exemptions from the Privacy Act. This is contrary to the weight of submissions to the Privacy Act Review, and the view expressed in the Review's Final Report, which indicated that the blanket exclusion of political parties from information privacy obligations was inconsistent with community expectations and unnecessary to uphold rights to freedom of political expression and political communication. The basis for the exemption of political parties traditionally rested on freedom of political communication and was introduced to 'enhance the operation of the electoral and political process in Australia'.[147] However, the Privacy Review reported that those who made submissions

[144] Submission 5 (Tasmanian Legal Aid) 4.
[145] Submission 8 (Meg Webb MLC).
[146] See discussion in ALRC, *Traditional Rights and Freedoms – Encroachments by Commonwealth Laws* (Report 129, 2016) [8.53]–[8.82].
[147] Privacy Act Review Report 2022 72.

considered that the political exemption was not achieving its purpose and was serving to undermine the integrity of the democratic electoral process'.[148] As a result, the Review proposed a more qualified exemption. Such an exemption would be confined to acts and activities relating to political processes, would apply only when a 'fair and reasonable' test is met (discussed further in Part 5 of this Report) and would impose obligations on political entities in terms of information handling, disclosure and opt-out mechanisms, and notification of data breach. It is also noted that the political party exemption is also contrary to the views of the Australian Law Reform Commission from 2008 that, 'There are compelling policy reasons – as well as strong stakeholder support – for applying privacy obligations to registered political parties and political acts and practices'.[149]

3.6.4 The TLRI notes the concern raised in the submission of Meg Webb MLC about the adequacy of privacy protections applying to government contractors. The TLRI observes that government contractors are bound by the PIPA as 'personal information custodians' where they have entered a contract with a public authority and the contract involves the collection, use or storage of personal information (see [3.2.4] above).[150] This means avenues for complaints against contractors in relation to breaches of PIPPs are available in these circumstances (although these could be strengthened further, as outlined in Part 8 of this Report). The PIPA provisions relating to government contractors' obligations are similar to, and in some ways stronger than, those found in other State and Territory jurisdictions (see [3.3.3] above). On this basis, the TLRI does not recommend changes to the obligations of government contractors, or agencies contracting with them, but notes that further consideration of the guidance that government agencies provide to contractors may be appropriate.

3.7 Recommendations

3.7.1 The TLRI makes no recommendations regarding the bodies subject to the PIPA.

[148] Privacy Act Review Report 2022 [8.2].
[149] ALRC, *Privacy* [41.41].
[150] PIPA s 3 (definition of 'personal information custodian' and 'personal information contract'); s 17.

Part 4

Scope and Application of the PIPA – Information Protected by the PIPA

4.1 Overview of this Part

4.1.1 This Part examines the scope of the *Personal Information Protection Act 2004* (Tas) ('PIPA') in terms of the information to which it provides protection. It considers:

- whether the definition of 'personal information', which dictates what information is subject to the Personal Information Protection Principles ('PIPPs') protections, requires amendment [4.2];
- whether any changes are required in relation to the types of personal information that receive greater protection than general personal information under the PIPA (such as sensitive information) [4.3]); and
- whether the gaps or exceptions in the PIPA, which provide some information with a lower level of protection, are appropriate [4.4].

4.2 Protection of 'personal information' in the PIPA

4.2.1 The Tasmanian PIPPs established in the PIPA generally apply to the protection of 'personal information'.[151] This sub-section discusses the definition of personal information and related matters.

The Tasmanian position

4.2.2 The PIPA defines 'personal information' as:[152]

> any information or opinion in any recorded format about an individual –
>
> (a) whose identity is apparent or is reasonably ascertainable from the information or opinion; and
>
> (b) who is alive or has not been dead for more than 25 years.

[151] See the discussion of health information and sensitive information for an example of where information may be covered by the PIPPs but may not be personal information; for example, genetic information (see below at [4.7.8]).
[152] PIPA s 3 (definition of 'personal information').

Information or opinion 'about an individual'

4.2.3 The requirement that information be 'about an individual' has been interpreted as requiring that the individual in question is 'a subject matter of the information or opinion'.[153] It is unclear whether this includes technical information about an individual's use of devices or networks and whether it includes information about inferences and predictions regarding individuals as members of a class or group.[154]

Identity is 'reasonably ascertainable'

4.2.4 While the PIPA specifies that personal information can include information which does not name or identify the person directly, but where the information makes the person's identity 'reasonably ascertainable',[155] 'reasonably ascertainable' is not defined in the PIPA, judicial interpretations, or guidance published by the Tasmanian Ombudsman.

De-identification and pseudonymisation

4.2.5 The PIPA addresses the possibility of the de-identification of personal information in several places. For example, the PIPPs place obligations on personal information custodians to take reasonable steps to permanently de-identify personal information if it is no longer needed for any purpose (PIPP 4(2)) and to take reasonable steps to permanently de-identify certain types of health information before it is disclosed (PIPP 10(5)). Both obligations are discussed further in this part of the Final Report.

4.2.6 De-identification is not defined in the PIPA, and the extent of de-identification required to meet these obligations is unclear. For instance, it is not clear whether it must no longer be technically possible to identify the person at all, or whether it only requires that the identity of the person no longer be 'reasonably ascertainable'.

Deceased persons

4.2.7 The PIPA protects the personal information of persons for up to 25 years after their death.[156] A deceased person's next of kin can exercise the deceased person's personal information rights, including amending and correcting the personal information in question. This aligns with rights provided by the *Right to Information Act 2009* (Tas).[157]

[153] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 [63].
[154] See, eg, OAIC, *Privacy Act Review: Submission by the Office of the Australian Information Commissioner* (Issues Paper, 11 December 2020) ('*Submission to Privacy Act Review*') 27–33.
[155] PIPA s 3 (definition of 'personal information').
[156] This provision was introduced in the *Personal Information Protection Amendment Act 2009* (Tas).
[157] *Right to Information Act 2009* (Tas) ss 5 (definition of 'personal information'); 5(6). Note that under PIPP 2(4), health services are able to disclose a person's health information, including the health information of a deceased person, to someone who is related to or responsible for them on compassionate grounds: PIPA, sch 1.

The position in other jurisdictions

Information or opinion 'about an individual'

4.2.8 The Commonwealth *Privacy Act 1988* (Cth) ('Privacy Act') adopts a related, but not identical, definition of 'personal information' to that found in the PIPA. The Privacy Act defines 'personal information' as:

> information or an opinion about an identified individual, or an individual who is reasonably identifiable:
>
> (a) whether the information or opinion is true or not; and
>
> (b) whether the information or opinion is recorded in a material form or not.[158]

4.2.9 Hence, the Privacy Act, like the PIPA, specifies that personal information is information or an opinion 'about an … individual'. This reflects the definition used in other jurisdictions.[159] However, unlike the PIPA, the Privacy Act and the relevant legislation in Victoria, Queensland, and the ACT specifies that it does not matter if the information or opinion is true,[160] and specifies that it does not matter whether the information is recorded in a material form.[161] The Office of the Australian Information Commissioner ('OAIC') provides some common examples of 'personal information', such as 'an individual's name, signature, address, telephone number, date of birth, medical records, bank account details, employment details and commentary or opinion about a person'.[162]

4.2.10 It is notable that the European Union's *General Data Protection Regulation 2106/679* ('GDPR') defines personal information (which it terms 'personal data') more broadly than either the PIPA or the Privacy Act, stating that personal data are 'any information *relating to* an identified or identifiable natural person'.[163] The Court of Justice of the European Union has clarified that 'relating

---

[158] *Privacy Act 1988* (Cth) s 6.

[159] *Privacy and Personal Information Protection Act 1998* (NSW) ('PPIP Act') s 4(1). It is noted that, in NSW, health information within the meaning in the *Health Records and Information Privacy Act 2002* is not included in the definition of personal information (s 4A) except where provided; *Information Privacy Act 2009* (Qld) s 12; *Information Privacy Act 2014* (ACT) s 8; *Privacy and Data Protection Act 2014* (Vic) s 3. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) has been passed but not commenced. This replaces s 12 with a definition of personal information that is consistent with the definition in the *Privacy Act 1988* (Cth).

[160] Cf *Privacy Act 1988* (Cth) s 6 (definition of 'personal information'):

'information or an opinion about an identified individual, or an individual who is reasonably identifiable:

(a) whether the information or opinion is true or not; and

(b) whether the information or opinion is recorded in a material form or not; *Information Privacy Act 2009* (Qld) s 12; *Information Privacy Act 2014* (ACT) s 8; *Privacy and Data Protection Act 2014* (Vic) s 3. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) has been passed but not commenced.

[161] Cf *Privacy Act 1988* (Cth) s 6. Note that while the some of the APPs apply to a record of personal information (eg APP 6), the definition of personal information can include information shared verbally: see OAIC, '*What is Personal Information?*' (Web Page, 5 May 2017) <https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/>. This is also the position under the *Privacy and Personal Information Protection Act 1998* (NSW) s 4, the *Information Privacy Act 2009* (Qld) s 12 and the *Information Privacy Act 2014* (ACT) s 8. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) has been passed but not commenced.

[162] OAIC, *Australian Privacy Principles Guidelines: Chapter B: Key Concepts* (2022) <https://www.oaic.gov.au/privacy/australian-privacy-principles/australian-privacy-principles-guidelines/chapter-b-key-concepts>.

[163] *General Data Protection Regulation 2106/679* ('GDPR') art 4(1) (emphasis added).

to' encompasses information that relates to an individual in terms of the content, purpose, or result/effect of the information.[164]

Identity is 'reasonably ascertainable'

4.2.11 The Commonwealth Privacy Act definition of personal information uses the term 'reasonably identifiable', rather than the PIPA term 'reasonably ascertainable'. 'Reasonably identifiable' is also used in the ACT;[165] 'reasonably ascertainable' is used in New South Wales ('NSW'),[166] Queensland,[167] Victoria,[168] and the Northern Territory.[169] Guidance on the interpretation of the Privacy Act published by the OAIC states that the term 'reasonably' requires a consideration of 'whether, objectively speaking, it is reasonable to expect that the subject of the information could be identified'.[170] This assessment requires 'a contextual consideration of the particular circumstances', which includes:

- 'the nature and amount of information';
- 'who might have access to the information'; and
- 'the other information that is available, and the practicability of using that information to identify an individual'.[171]

De-identification and pseudonymisation

4.2.12 Like the PIPA, the Privacy Act obliges regulated entities to take reasonable steps to 'de-identify' personal information in certain circumstances.[172] There are provisions that address de-identification in other Australian jurisdictions.[173] Unlike the PIPA and the Victorian and ACT legislation, the Privacy Act provides some explanation of what constitutes 'de-identified' personal information, holding that personal information is de-identified 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable'.[174] This is also the definition contained in the equivalent Victorian and ACT legislation.[175] Under the Privacy Act, de-identified

[164] See *Peter Nowak v Data Protection Commissioner* (Court of Justice of the European Union, C-434/16, ECLI:EU:C:2017:994, 20 December 2017); *YS v Minister voor Immigratie, Integratie en Asiel and Minister voor Immigratie, Integratie en Asiel v M, S,* (Court of Justice of the European Union, C-141/12 and C-372/12, ECLI:EU:C:2014:2081, 17 July 2014).
[165] *Information Privacy Act 2014* (ACT) s 8.
[166] *Privacy and Personal Information Protection Act 1998* (NSW) ('PPIP Act') s 4(1).
[167] *Information Privacy Act 2009* (Qld) s 12. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) s 12 replaces the definition of personal information with a definition that is consistent with the definition in the *Privacy Act 1988* (Cth) (yet to be commenced).
[168] *Privacy and Data Protection Act 2014* (Vic) s 3.
[169] *Information Act 2002* (NT) s 4A.
[170] OAIC, *What is Personal Information* (Guidance Document, May 2017) 8.
[171] Ibid.
[172] See, eg, APP 11.2, 4.3, 6.4.
[173] *Information Privacy Act 2009* (Qld) schs 3 and 4; *Information Privacy Act 2014* (ACT) sch 1; *Privacy and Data Protection Act 2014* (Vic) sch 1; *Privacy and Personal Information Protection Act 1998* (NSW) s 27B; *Information Act 2002* (NT) sch 2). It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces sch 3 (Information Privacy Principles) and sch 4 (National Privacy Principles) with a new sch 3 (Queensland Privacy Principles) (yet to commence).
[174] *Privacy Act 1988* (Cth) s 6(1) (definition of 'de-identified').
[175] *Information Privacy Act 2014* (ACT) s 18; *Privacy and Data Protection Act 2014* (Vic) s 3.

information is not 'personal information'.[176] In NSW, Queensland, and the Northern Territory ('NT'), the term 'de-identification' is not defined.[177]

4.2.13 The European Union's GDPR does not use the term 'de-identification' and instead uses terms such as 'anonymisation' and 'pseudonymisation' on the basis that these promote clarity in legal standards.[178] Relevantly, the GDPR's protective scope covers information which has been subject to 'pseudonymisation'; that is 'the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject *without the use of additional information*'.[179] Pseudonymisation is distinguished from complete anonymity in the sense that pseudonymised data could still be attributed to a person and is therefore protected. However, if personal data is processed in such a way that the individual is not, or is no longer, identifiable at all—not even with the help of additional information—then it becomes anonymous data and is not protected by the GDPR.[180]

Deceased persons

4.2.14 Unlike the PIPA, the Privacy Act does not apply to personal information about deceased persons, unless the information is also about a living person.[181] In contrast, privacy legislation in NSW, Victoria, and the NT protects the personal information of deceased individuals. The legislation in NSW and Victoria protects that information for a longer period, of not more than 30 years after the individual's death,[182] while the legislation in the NT applies to 'a deceased individual within the first 5 years after death'.[183]

4.3 The Commonwealth Privacy Act Review

4.3.1 The Commonwealth Privacy Act Review Report proposed a number of changes to the definition of 'personal information' in the Privacy Act that are relevant to this review of Tasmanian privacy protection.

Information or opinion 'about an individual'

4.3.2 In its Final Report, the Review proposed that the phrase 'about an individual' in the definition of personal information in the Privacy Act—which is also found in the PIPA—be changed to the phrase 'relates to an individual'.[184]

4.3.3 This proposal drew on the Australian Competition and Consumer Commission's ('ACCC') *Digital Platforms Inquiry* ('DPI') report, which recommended that the definition of 'personal

[176] OAIC, Australian *Privacy Principles Guidelines* [B.62].
[177] It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld includes a definition of de-identify that is consistent with the *Privacy Act 1988* (Cth) in sch 5 (yet to commence).
[178] OAIC, *Privacy Act Review Issues Paper Submission* <https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/part-2-definition-of-personal-information> [2.35].
[179] GDPR art 4 (emphasis added).
[180] GDPR recital 26.
[181] *Privacy Act 1988* (Cth) s 5; OAIC, 'What is Personal Information?'.
[182] See *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3)(a); *Health Records Act 2001* (Vic) s 3. Note that the Northern Territory extends protection for deceased persons for 5 years: *Information Act 2002* (NT) s 4 (definition of 'person').
[183] *Information Act 2002* (NT) s 4.
[184] Privacy Act Review Report 2022 Proposal 4.1.

information' in the Privacy Act be amended in order to clarify that it applies to technical data, such as 'IP addresses, device identifiers, location data, and any other online identifiers that relate to an identified individual'.[185] Such a change was considered necessary due to legal uncertainty following the Federal Court of Australia's decision in *Privacy Commissioner v Telstra Corporation Ltd* ('the Grubb case').[186]

4.3.4 In its Final Report, the Privacy Act Review asserted that substituting 'about' with 'relates to' was not intended to significantly expand the already expansive scope of the definition of personal information, but rather to clarify—in conjunction with its other proposals about amending the definition of personal information—that 'personal information' includes 'technical information, inferred information and any other information where that information relates to the individual, in the sense that it can be seen to provide details about their activities or their identity and the connection is not too tenuous or remote'.[187] The Review also observed that this change would bring the Privacy Act into alignment with international data protection regimes, such as the GDPR, and other Commonwealth legislation, such as Consumer Data Right ('CDR').[188]

4.3.5 This proposal was supported by a wide range of respondents to the Privacy Act Review's Discussion Paper, with a smaller number of submitters raising concerns about the breadth of the phrase 'relates to' or the potential compliance costs or regulatory burden of an expanded definition.[189] In its report, the Review expressed the view that these concerns should be addressed when the reform was enacted. This could be achieved by ensuring, through the drafting of the provision, explanatory materials and OAIC guidance, that the definition of 'personal information' is 'appropriately confined to where the connection between the information and the individual is not too tenuous or remote'.[190]

4.3.6 In response to stakeholder feedback that there was 'continued confusion about the scope and content of the definition' of personal information,[191] the Review also proposed the inclusion in the Privacy Act of a non-exhaustive list of information which may constitute 'personal information'. The purpose of the list would be to assist Australian Privacy Principles ('APPs') entities to identify the types of information that could fall within the definition, which could then be supplemented with more specific examples in the explanatory materials and OAIC guidance.[192] According to the Review, appropriate inclusions for the list were:

- 'name, date of birth or address';
- 'an identification number, online identifier or pseudonym';
- 'contact information';
- 'location data';
- 'technical or behavioural data relating to an individual's activities, preferences, or identity';
- 'inferred information, including predictions of behaviour or preferences, and profiles generated from aggregated information'; and
- 'one or more features specific to the physical, genetic, mental, behavioural, economic, cultural or social identity or characteristics of a person'.[193]

[185] ACCC, *Digital Platforms Inquiry Report* 458 ('*DPI Report*').
[186] (2017) 249 FCR 24; ACCC, *DPI Report* 459; and see Privacy Act Review Report 2022 25.
[187] Privacy Act Review Report 2022 25.
[188] Ibid 25 and citing Privacy Act Review Discussion Paper 26–27.
[189] Ibid 26.
[190] Ibid Proposal 4.1.
[191] Ibid 28.
[192] Ibid Proposal 4.2.
[193] Privacy Act Review Report 2022 29.

Identity is 'reasonably identifiable'

4.3.7 The Privacy Act Review considered whether there was a need for clarification of the second limb of the definition of personal information; namely, that an individual must be 'identified or reasonably identifiable'. It noted that submitters had reported difficulty in determining the point at which an individual becomes identifiable and in understanding the standard that should be used to satisfy the 'reasonably identifiable' requirement.[194] The Review also noted that the growth in large datasets about individuals has increased the risk that unidentified information will become identified when it is linked to other information.[195]

4.3.8 The Review proposed that the Privacy Act should be amended to insert a non-exhaustive list of circumstances to which APP entities will be expected to have regard in assessing whether identity is 'reasonably identifiable'.[196] It noted that whether a person is reasonably identifiable will depend on a number of factors, including the context in which the information exists, the means reasonably likely to be used to identify someone, and current data processing practices, among others.[197]

4.3.9 The Review proposed a list of five 'circumstances' that could assist APP entities to assess reasonable identifiability:

- 'the nature and volume of the information';
- 'who holds or has access to the information';
- 'how and why the information is collected, used, stored and disclosed';
- 'the other information that is available (or known) to the recipient, and the practicability of using that information to identify the individual'; and
- 'the context in which information is handled, including the context into which information will be disclosed'.[198]

4.3.10 In its response to the Privacy Act Review Final Report, the Commonwealth Government agreed in-principle with the proposals to change 'about' to 'relates to' and to introduce non-exhaustive lists of the types of information that may be personal information and of circumstances to which APP entities are expected to have regard when assessing reasonable identifiability. The Commonwealth Government expressed an intention to 'consult further on how the definition of personal information may improve understanding of when information relates to an individual who is identified or reasonably identifiable'.[199]

De-identification and pseudonymisation

4.3.11 In the Privacy Act Review Final Report, the Review observed that APP entities have difficulty meeting the de-identification requirements in the APPs because they may not understand the standard of de-identification required.[200] Citing the ACCC's DPI Report, the Review emphasised 'the importance

[194] Ibid 32.
[195] Ibid 31.
[196] Ibid Proposal 4.4.
[197] Ibid 34 and citing a number of submissions.
[198] Ibid 35.
[199] Government Response 5.
[200] Privacy Act Review Report 2022 36.

of robust deidentification standards' in the context of growing availability of identification due to ongoing technological advances and the increasing volumes of data in circulation.[201]

4.3.12 Based on the submissions it had received, the Review concluded that replacing 'de-identification' with an irreversible standard of anonymisation, which had been discussed in its Discussion Paper,[202] was not practically achievable. The Review proposed instead that the definition of 'de-identified' in the Privacy Act be amended 'to make it clear that de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context'.[203] This involves acknowledging that de-identification is subject to circumstances and context, and that past de-identification may not be adequate to ensure continued de-identification when circumstances change (such as where new linkable information is added).[204] The Government agreed in-principle with this proposal, meaning it intended to further examine whether and how it could be implemented in consultation with APP entities.[205]

4.3.13 The Review also recommended that protections under several APPs be extended to de-identified information, in line with developments in overseas jurisdictions. These recommendations are discussed in Part 7, below.

4.3.14 The Review recommended that there be further consultation on the introduction of a criminal offence (with appropriate exceptions) for 'malicious re-identification' of de-identified information in circumstances where there is an intention to harm another or obtain an illegitimate benefit, either by an external person or by an APP entity acting maliciously.[206] The Commonwealth Government agreed with this proposal.[207]

4.3.15 Finally, the Review recommended the introduction of a prohibition on APP entities from re-identifying information that it obtained from a source other than the individual to whom the information relates, with some limited exceptions (such as where the re-identified information was de-identified by the APP entity itself, in which case the entity should simply comply with the APPs).[208] In responding to this proposal, the Commonwealth Government said it 'generally agrees with the policy intent of protecting de identified [sic] information from unauthorised re-identification' and would further consider how this objective may be achieved.[209]

Deceased persons

4.3.16 The Privacy Act Review considered the inconsistency between Commonwealth and State and Territory rules regarding deceased persons, noting that the Australian Law Reform Commission ('ALRC') recommended in 2008 that the Privacy Act 'be extended to cover information about deceased

[201] Ibid; see ACCC, *Digital Platforms Inquiry* 476.
[202] Privacy Act Review Discussion Paper Proposal 2.5.
[203] Ibid Proposal 4.5
[204] Ibid 37. The Review also contemplated that technological developments might in future require the development of APP codes (discussed in Part 5 of this Report) to deal with 'technically complex and evolving uses of personal information and de-identified information': ibid.
[205] Government Response.
[206] Privacy Act Review Report 2022 Proposal 4.7. The Review observed that criminal offences for re-identification of de-identified information released by government agencies are provided for in the *Data Availability and Transparency Act 2022* (Cth), meaning the Review's proposal was confined to strictly malicious re-identification: ibid 40.
[207] Government Response 4.
[208] Privacy Act Review Report 2022 Proposal 4.8.
[209] Government Response 5.

persons'.[210] In its Final Report, the Review declined to propose amendments to the Privacy Act on this issue, instead noting that the Standing Council of Attorneys-General agreed in December 2022 to 'provide drafting instructions to the Parliamentary Counsel's Committee for the development of uniform model legislation for a national access scheme for digital records after death or incapacity'.[211] This is consistent with prior recommendations[212] and efforts made towards developing a nationally consistent approach to accessing digital records upon death or incapacity.[213] The TLRI notes that this project was discontinued in late-2023, on the basis of the view that uniform legislation would not be appropriate in light of the complex interaction of legal frameworks and the variety of digital record holders. The Standing Council of Attorney-General agreed that 'there is merit in allowing for digital record holders to respond to these issues in a way that is tailored to their services'.[214]

4.4 Consultation

4.4.1 The TLRI Issues Paper invited submissions on the scope of the definition of 'personal information' in the PIPA in the following terms:

> Should the definition of 'personal information' be changed? Should it be consistent with the definition in the Privacy Act, or with the definition of personal data in the European Union's GDPR?[215]

Information or opinion 'about an individual'

4.4.2 The Ombudsman expressed the view that a 'wholesale review of the legislation would be beneficial', including reconsideration of the definition of personal information.[216]

4.4.3 Academics in the Centre for Law and Genetics at the University of Tasmania, Professor Margaret Otlowski, Emeritus Distinguished Professor Dianne Nicol, and Dr Lisa Eckstein, submitted that they saw merit in making the definition of 'personal information' in the PIPA 'as consistent as possible' with the Privacy Act. They noted the proposal in the Privacy Act Review Final Report to replace the word 'about' with the words 'relates to' and agreed that this would address uncertainty arising from the Grubb case (see [4.3.3]), align the definition more closely with the GDPR definition, and better highlight the need for there to be a relationship between the information and the individual in order for it to constitute 'personal information'.[217]

[210] Privacy Act Review Report 2022 41 and citing ALRC, *Privacy* 377.
[211] Ibid 42 and citing Attorney-General's Department, Standing Council of Attorneys-General, *Communiqué* (9 December 2022) 4.
[212] NSW Law Reform Commission, *Access to Digital Records Upon Death or Incapacity* (Report No 147, December 2019) 81–83.
[213] Council of Attorneys-General, *Communiqué* (27 July 2020) <https://www.ag.gov.au/about-us/publications/council-attorneys-general-communique-july-2020>; Meeting of Attorneys-General, *Communiqué* (31 March 2021) <https://www.ag.gov.au/about-us/who-we-are/committees-and-councils/meeting-attorneys-general>.
[214] Standing Council of Attorneys-General, *Communiqué* (22 September 2023) <https://www.ag.gov.au/sites/default/files/2023-09/scag-communique-september-2023_0.pdf>.
[215] Issues Paper Part 2, Question 2.4.
[216] Submission 4 (TasCOSS).
[217] Submission 17 (Centre for Law and Genetics).

Identity is 'reasonably ascertainable', de-identification, and pseudonymisation

4.4.4 The Centre for Law and Genetics team also supported the Privacy Act Review's proposals relating to de-identification and pseudonymisation. They recommended that Tasmania follow the lead of the Commonwealth Review in seeking to address uncertainties in the operation of the 'reasonable identifiability' test in relation to the Review's proposals to:

- introduce a list of factors for APP entities to consider when determining whether an individual is reasonably identifiable (see above [4.3.9]);
- amend the definition of 'de-identify' to clarify that whether or not de-identified information remains de-identified depends on context (see above [4.3.12]); and
- extend protections to de-identified information that are proportionate to the risk of the information being re-identified (see above [4.2.13]–[4.3.13]).

Deceased persons

4.4.5 No submissions to this project addressed the inclusion of deceased persons, or the duration of protection of personal information about deceased persons, in the PIPA.

4.5 The TLRI's view

Information or opinion 'about an individual'

4.5.1 The TLRI considers that the proposed changes to the Privacy Act definition of personal information in the Privacy Act Review Report, such as changing 'about' to 'relates to' in the definition of 'personal information' and introducing a non-exhaustive list of information that may fall within the definition of personal information, would also be appropriate amendments to the PIPA. Such changes would not significantly expand the scope of the legislation but would clarify that privacy protections are limited to personal information that has a genuine connection to an individual and affirm the inclusion of technical data in the definition. These reforms would also promote consistency with overseas jurisdictions (notably the European Union) and, if enacted at the Commonwealth level, within Australia.

Identity is 'reasonably identifiable'

4.5.2 The TLRI also considers that it may be appropriate to change the words 'reasonably ascertainable' to 'reasonably identifiable' in the definition of 'personal information' in the PIPA. This would promote consistency between the Tasmanian and Commonwealth legislation. It is also the approach that will be implemented in Queensland, once the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) comes into force. If the Privacy Act Review Report's proposals are implemented, it would also pave the way for the insertion into the PIPA of a non-exhaustive list of circumstances to which PIPA personal information custodians will be expected to have regard in assessing whether identity is 'reasonably identifiable'.[218] This list could mirror the list inserted in the

[218] Privacy Act Review Report 2022 Proposals 4.4, 4.6.

Privacy Act, and would provide valuable but flexible guidance for PIPA personal information custodians.

4.5.3 The TLRI observes that adopting the term 'reasonably identifiable' in the PIPA would make the terminology used in relation to personal information in PIPA inconsistent with the *Right to Information Act 2009* (Tas), so this issue would need to be considered in the reform process.

De-identification and pseudonymisation

4.5.4 The TLRI shares the view of other reform and review bodies that modern technology can make it easier to draw links that identify and re-identify de-identified information, due to increasingly sophisticated forms of analysis and increased access to other sources of personal information. The TLRI is also of the view that bodies subject to the PIPPs, and the individuals whose personal information is held by those bodies, would benefit from further guidance in the PIPA on the meaning and practice of de-identification.

4.5.5 On this basis, the TLRI is of the view that the PIPA should be amended to insert a definition of 'de-identified' that aligns with the definition of 'de-identified' set out in the Privacy Act Review Report. The purpose of the proposed amendments was to clarify that de-identification is not a one-off process, that it should be informed by best practice, and that de-identification is subject to circumstances and context.[219] The TLRI considers that this definition would be most appropriate in light of the growing capacity for entities to identify and re-identify information. As noted, the Commonwealth Government has also agreed in-principle with this proposal.

4.5.6 The TLRI also notes the proposed amendments to the Privacy Act to:

- introduce a criminal offence for 'malicious re-identification' of de-identified information where there is an intention to harm or obtain an illegitimate benefit may also be appropriate in future;[220] and/or
- introduce a prohibition on PIPA personal information custodians from re-identifying information obtained from a source other than the individual to whom the information relates.[221]

4.5.7 Aligned with the TLRI's view about the importance of consistency with other jurisdictions, and the fact that these matters were not raised in the Issues Paper, nor were they the subject of submissions on their significance in the Tasmanian context, further consideration and consultation on the need and appropriateness of introducing comparable provisions in the PIPA may be appropriate.

4.5.8 The Issues Paper for this project observed that the requirement in PIPP 10 for personal information custodians to take reasonable steps to permanently de-identify health information before disclosing it for research or statistical analysis on public health or safety or running a health service[222] may impact the development and use of pseudonymous datasets for health research which involves

[219] Ibid Proposal 4.6.
[220] Ibid Proposal 4.7. This proposal reflects the powers of the Safety Commission relating to publishing private or identifying information about an individual with malicious intent to cause serious harm, see eSafety Commissioner, *Our Legislative Functions* (Web Page, 22 December 2023) <https://www.esafety.gov.au/about-us/who-we-are/our-legislative-functions>.
[221] Privacy Act Review Report 2022 Proposal 4.8. The Review specified some exceptions to this prohibition; namely, where 'the re-identified information was de-identified by the APP entity itself—in this case, the APP entity should simply comply with the APPs in the ordinary way' and where 'the re-identification is conducted by a processor with the authority of an APP entity controller of the information': ibid.
[222] PIPA sch 1, PIPP 10(5); see [5.2.9] below.

comparing the characteristics within a selected sample population.[223] Submissions in response to the Issues Paper did not express a similar concern.

Deceased persons

4.5.9 The TLRI observes that there currently exist only minor differences in the treatment of the personal information of deceased persons in State and Territory information privacy legislation, and the recent agreement of the Standing Council of Attorneys-General that uniform legislation would not be an appropriate solution to concerns about access to digital records after death.[224] The jurisdictional differences relate to the duration of preservation of the privacy of that information, and the TLRI does not consider that these inconsistencies necessitate any changes to the PIPA.

4.6 Recommendations

Recommendation 1: The definition of 'personal information' in the PIPA should be amended to:

- replace 'about' with 'relating to'; and
- introduce a non-exhaustive list of information that may fall within the definition of personal information.

Recommendation 2: Further consideration should be given to:

- amending the definition of 'personal information' by replacing 'reasonably ascertainable' with 'reasonably identifiable'; and
- providing further guidance for personal information custodians by inserting a non-exhaustive list of circumstances to which PIPA personal information custodians will be expected to have regard in assessing whether identity is 'reasonably identifiable'.

Recommendation 3: The PIPA should be amended to insert a definition of 'de-identified' that is consistent with the definition in the *Privacy Act 1988* (Cth) and that clarifies that 'de-identification is a process, informed by best available practice, applied to personal information which involves treating it in such a way such that no individual is identified or reasonably identifiable in the current context'.[225]

Recommendation 4: Further consideration should be given to whether the PIPA should be amended to:

- introduce a criminal offence for 'malicious re-identification' of de-identified information where there is an intention to harm or obtain an illegitimate benefit;[226] and/or
- introduce a prohibition on PIPA personal information custodians from re-identifying information obtained from a source other than the individual to whom the information relates.[227]

[223] Note that the assignment, use, and disclosure of Commonwealth Government healthcare identifiers is also regulated under the *Healthcare Identifiers Act 2010* (Cth).
[224] Standing Council of Attorneys-General, *Communiqué* (22 September 2023).
[225] Privacy Act Review Report 2022 Proposal 4.5.
[226] Ibid Proposal 4.7.
[227] Ibid Proposal 4.8.

4.7 Types of information given additional protection in the PIPA

The Tasmanian position

4.7.1 The PIPA distinguishes several categories of information that are subject to greater or lesser protection than personal information generally. These include basic information, health information, sensitive information, employee information, and law enforcement information. This sub-section discusses information that is subject to greater or additional protection.

Sensitive information

4.7.2 Under the PIPA, certain types of personal information are classed as 'sensitive information'; namely,[228]

> (a) personal information or an opinion relating to personal information about an individual's –
>
> (i) racial or ethnic origin; or
>
> (ii) political opinions; or
>
> (iii) membership of a political association; or
>
> (iv) religious beliefs or affiliations; or
>
> (v) philosophical beliefs; or
>
> (vi) membership of a professional or trade association; or
>
> (vii) membership of a trade union; or
>
> (viii) sexual preferences or practices; or
>
> (ix) criminal record; and
>
> (b) health information about an individual.

4.7.3 The handling of personal information that is 'sensitive information' is generally subject to more, or more stringent, requirements under the PIPPs. First, use or disclosure of sensitive information by a personal information custodian is only permitted where the use or disclosure is *directly* related—rather than related, *simpliciter*—to the primary purpose for which the information was collected.[229] Secondly, the collection of sensitive information generally requires the consent of the individual concerned, except where the PIPA specifies otherwise. For example, the Act provides exceptions where collection is required or permitted by law, or where it is necessary to prevent or lessen serious and imminent threat to life or health. The treatment of sensitive information in the PIPPs is discussed in more detail in Part 5 of this Report.[230]

[228] PIPA s 3.
[229] PIPA sch 1, PIPP 2(1).
[230] PIPA sch 110.

Health information

4.7.4 As noted above, health information is one category of personal information that the PIPA characterises as 'sensitive information'.[231] The PIPA defines health information by reference to two categories: (i) the nature of the information; and (ii) where the information has been collected.

4.7.5 In relation to the first category, the PIPA defines health information to mean 'personal information or opinion about':

- the physical, mental, or psychological health at any time of an individual;
- a disability at any time of the individual;
- an individual's expressed wishes about the future provision of health services to them; and
- a health services provided, or to be provided, to an individual.[232]

4.7.6 It is unclear why this definition refers to 'personal information or opinion' about a person's health, given that the definition of 'personal information' encompasses an opinion about an individual.[233]

4.7.7 In relation to the second category, the definition of 'health information' encompasses:[234]

- other personal information collected in providing a health service;[235]
- other personal information collected in connection with body part, organ, or body substance donation; and
- genetic information about an individual that is or may be predictive of the individual's or their descendants' health.[236]

4.7.8 The description of genetic information is the only form of health information defined in the PIPA that does not use the term 'personal information'.[237] It is therefore unclear whether that aspect of the definition is broader, in the sense that it may include information which is not personal information.

---

[231] PIPA s 3 (definition of 'sensitive information', para (b)).
[232] PIPA s 3 (definition of 'health information', para (a)).
[233] PIPA s 3 (definition of 'personal information').
[234] PIPA s 3 (definition of 'health information').
[235] A 'health service' is defined in s 3 as 'an activity, other than a prescribed activity, performed in relation to an individual that is intended or claimed by the individual or the person performing it—
(a) to assess, maintain or improve the individual's health; or
(b) to diagnose the individual's illness, injury or disability; or
(c) to treat the individual's illness, injury or disability or suspected illness, injury or disability;
(d) to dispense on prescription a drug or medical preparation; or
(e) to provide a disability service, palliative care service or aged care service; or
(f) to provide a prescribed service or a prescribed class of service in conjunction with any activity referred to in paragraph (a), (b), (c), (d) or ©'
Note that a 'health service' is defined differently in the *Health Complaints Act 1995* (Tas). See discussion below at [10.17.2].
[236] PIPA s 3 (definition of 'health information' paras (b), (c) and (d)).
[237] This is also the case under the *Privacy Act 1988* (Cth) and in the ACT. In contrast, in the Northern Territory, health information is defined to include 'personal information that is genetic information about a person …', *Information Act 2002* (NT) s 4. This is also the position in Victoria, *Health Records Act 2001* (Vic) s 3. In New South Wales, genetic information is included in the definition of personal information in the *Health Records and Information Privacy Act 2002* (NSW) s 5(2). Genetic information is not referred to in the *Information Privacy Act 2009* (Qld). However, this will be included on the commencement of the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) (Schedule 5 amendment).

It is also unclear whether it is confined to information that only relates to an individual that is predictive of the individual's or their descendants' health or whether it also includes information about that individual's genetic relatives, which may be predictive of that individual's own health.

4.7.9 As a category of sensitive information, health information is subject to the additional protections under the PIPPs described at [4.7.3] above. However, certain exceptions to PIPA restrictions are available in relation to health information that do not apply to other types of sensitive information.

4.7.10 For example, under PIPP 2, a health service can disclose health information about an individual to a relative or responsible person for certain specified purposes where the individual is unable to give or communicate consent.[238]

4.7.11 PIPP 10 also permits the collection of health information without the individual's consent for several reasons, including where:

- the collection is necessary to provide a health service to the individual;[239]
- it is impracticable to seek such consent and the collection is for the purpose of research relevant to public health or public safety, compiling or analysing statistics relevant to public health or public safety, or managing, funding or monitoring a health service;[240] or
- the collection is from an individual about another person without the person's consent[241] and the collection is necessary to provide a health service to the individual and the information is relevant to the individual's social or family history.[242]

4.7.12 These exceptions are discussed in detail in Part 5 of this Report.

The position in other jurisdictions

4.7.13 The PIPA definition of sensitive information is similar to the definition in the Commonwealth Privacy Act, as well as the definition in Victoria, Queensland, the ACT and the NT.[243] One point of difference is that the Privacy Act and the ACT legislation use the term 'sexual orientation or practices'

[238] PIPA sch 1, PIPP 2(4). This exception only applies where the disclosure is considered necessary to provide appropriate care or treatment to the individual or is made for compassionate reasons, and only to the extent reasonable and necessary for that purpose. Such disclosure is not permitted if it is contrary to a wish of the individual, either expressed by them or that the person providing the health service is aware, or could reasonably be expected to be aware of.

[239] PIPA sch 1, PIPP 10(3). The information must be collected as required by law (other than the PIPA) or in accordance with the professional confidentiality rules established by health or medical bodies which bind the personal information custodian: ibid.

[240] PIPA sch 1, PIPP 10(4). Collection is only permitted for these purposes where it is not possible for the purpose to be served by collecting non-identifying information, and the information is collected as required by law or in accordance with any professional confidentiality obligations: ibid. The personal information custodian must take reasonable steps to permanently de-identify health information collected for these purposes before disclosing it: ibid sch 1, PIPP 10(5).

[241] Or without complying with the requirements in PIPP 1(5): see [5.2.4] below.

[242] PIPA sch 1, PIPP 10(6).

[243] *Information Privacy Act 2009* (Qld) sch 5; *Information Privacy Act 2014* (ACT) sch 1; *Privacy and Data Protection Act 2014* (Vic) sch 1; *Information Act 2002* (NT) s 4.

to refer to sensitive information about individuals' sexuality, while the PIPA and other State and Territory legislation use more outdated language of 'sexual preferences or practices'.[244]

4.7.14 Further, the Privacy Act and the legislation in the ACT identify three additional forms of sensitive information relating to genetics and biometrics:[245]

- genetic information about an individual that is not otherwise health information;
- biometric information used for the purpose of automated biometric verification or biometric identification; and biometric templates.[246]

4.7.15 Biometric information is information relating to the physical attributes of an individual, such as their face, gait, fingerprints, signature, or voice. Biometrics are commonly used in technological applications to verify identity, such as through facial recognition or fingerprint sensors on Smartphones.[247]

4.7.16 The Privacy Act definition of 'health information',[248] and exceptions to the general prohibition on the collection of health information where a person is unable to give or communicate consent, where necessary for research and related activities, or where the information is about another person, are similar to those in the PIPA.[249] These are discussed in detail at [5.4] of this Report.

4.7.17 In the New South Wales *Privacy and Personal Information Protection Act 1998* (NSW), as noted, 'personal information' does not include health information, which is defined in Section 6 of the *Health Records and Information Privacy Act 2002* (NSW).[250] However, in relation to data breaches in Part 6A of the former, 'personal information' does include 'health information'.[251] The definition of health information is consistent with the Tasmanian definition.[252] 'Sensitive information' is also not defined in the NSW legislation.

4.8 Proposals in the Commonwealth Privacy Act Review

4.8.1 The Privacy Act Review Report proposed amendments to the definition of 'sensitive information' in the Commonwealth legislation to:

[244] *Privacy Act 1988* (Cth) s 6(1) (definition of 'sensitive information'); *Information Privacy Act 2014* (ACT) sch 1 (definition of 'sensitive information'); *Privacy and Data Protection Act 2014* (Vic) sch 1 (definition of 'sensitive information'); *Information Act 2002* (NT) s 4 (definition of 'sensitive information'); *Information Privacy Act 2009* (Qld) sch 5 (definition of 'sensitive information'); see [4.7.2] above for the PIPA definition.
[245] *Privacy Act 1988* (Cth) s 6; *Information Privacy Act 2014* (ACT) sch 1. It is noted that this will also be the Queensland position on the commencement of the *Information Privacy and Other Legislation Amendment Act 2023* (Qld).
[246] Biometric templates are the mathematical files that represent the individual's unique features in digital form. They are produced after the unique features of an individual are extracted from a sample (such as a photo of their face or a voice recording), analysed, and then converted into mathematical data.
[247] See Biometrics Institute, *Types of Biometrics* (Web Page, 2024) <https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/>.
[248] *Privacy Act 1988* (Cth) s 6FA.
[249] *Privacy Act 1988* (Cth) ss 16B, 95, 95A
[250] See (n 159) above.
[251] *Privacy and Personal Information Protection Act 1998* (NSW) s 59B.
[252] It is noted that 'personal information' is also defined in the *Health Records and Information Privacy Act 2002* (NSW) ('HRIP Act') s 5.

- include genomic information (which is related to, but distinct from, genetic information and about which submitters to the Review indicated there was some confusion);
- replace the word 'about' with the words 'relates to' for consistency with the proposed amended definition of 'personal information' discussed at [4.3.2]–[4.3.5]) above; and
- clarify that inferences about sensitive information (including inferences based on non-sensitive information) constitute sensitive information; for instance, where information that an individual downloaded a gay dating app to their phone is non-sensitive information, but if a marketer treats that as information about the individual's sexual orientation and uses it to market to the individual, it will constitute sensitive information.[253]

4.8.2 In its response to the Privacy Act Review Final Report, the Commonwealth Government stated that it agreed in-principle with these proposals, and this would include 'consideration of additional OAIC guidance' to 'assist with clarifying when an inference is made and the practical implications of how the APPs may apply to inferred' information.[254]

4.8.3 The Review also referred to the Final Report of the Australian Human Rights Commission's ('AHRC') Human Rights and Technology project, which had highlighted the significant privacy risks associated with some uses of biometric technology, including facial recognition technology in surveillance.[255] Drawing from examples in other jurisdictions, including the EU, the AHRC recommended numerous reforms, including:[256]

- creating express protections for human rights when facial recognition technology is used in certain types of decision-making (namely, in decision-making that impacts a person's legal or similarly significant rights and in circumstances where use of the technology poses a high risk to human rights, such as in policing and law enforcement). In this context, there is particular concern that errors in recognition can result in mis-identification of suspects, victims, or witnesses, and thereby infringe on the right to procedural fairness, among other rights. This can be distinguished from low-risk contexts, such as where the technology is used in a payment system at a café.[257]
- introducing a moratorium on the use of facial recognition technology until the kind of protections discussed in the above recommendation are in place;[258] and
- introducing a statutory cause of action for invasion of privacy (discussed in detail further below Part 11).[259]

4.8.4 The Privacy Act Review recommended that the Privacy Act be amended to require all APP entities to undertake 'Privacy Impact Assessments' for activities with high privacy risks prior to the commencement of the high-risk activity (or upon request by the OAIC).[260] This proposal is discussed further in [8.7.6]. Related to this, the Review recommended a coordinated approach across Government to consider the regulation of biometric technologies, including through 'enhanced risk assessment requirements' for facial recognition and other biometric technologies, including in relation to

[253] Privacy Act Review Report 2022 Proposal 4.9, 45.
[254] Government Response 6.
[255] Australian Human Rights Commission ('AHRC'), *Human Rights and Technology Final Report* (Final Report, 2021) ch 9; Privacy Act Review Report 2022 43.
[256] AHRC, *Human Rights and Technology Final Report* 116–23.
[257] Ibid Recommendation 19, 117, 119.
[258] Ibid Recommendation 20.
[259] Ibid Recommendation 21.
[260] Privacy Act Review Report 2022 124.

information that may not constitute personal information but nevertheless poses a risk to individuals.[261] The Commonwealth Government agreed with this proposal in its response to the Final Report.[262]

4.8.5 The Review also examined whether additional regulation of the handling of geolocation tracking data was required. It defined geolocation tracking data as 'personal information which shows an individual's precise geolocation which is collected and stored by reference to a particular individual at a particular place and time, and tracked over time'.[263] The Review cited evidence of public concern about the widespread collection of location data, especially precise geolocation data, and its potential implications in terms of revealing sensitive information or creating risks to personal safety.[264] On this basis, it proposed amendments to the Privacy Act to define geolocation tracking data and to recognise that the collection, use, disclosure, and storage of precise geolocation tracking data requires valid and informed consent. The proposal was confined to precise data and to tracking data; that is, 'data collected repeatedly over time to record movements or activity'.[265]

4.8.6 In its response to the Report, the Government agreed in-principle with this proposal and committed to further considering 'whether this should be included as a new sub-category of sensitive information'.[266]

4.9 Consultation

4.9.1 The TLRI Issues Paper posed one question about sensitive information:

> Are the other categories of information, including health and other forms of sensitive information, suitable?[267]

4.9.2 Several submissions in reply to the Issues Paper expressed concern about the collection, use, and disclosure of biometric information by public and private entities, and, more specifically, about the limitations of existing legal mechanisms for protecting individuals' privacy in these situations. Meg Webb MLC submitted that the PIPA should be amended to recognise biometric information as a form of 'sensitive information'. Ms Webb identified several recent instances of the use, or proposed use, of biometric data in Tasmania. These included:

- the Tasmanian Government's transmission of drivers licence photographs to the Commonwealth's National Driver Licence Facial Recognition Solution ('NDLFRS') in the absence of legislated privacy protections under Commonwealth law;[268]
- a Ministerial Directive to the Tasmanian Liquor and Gaming Commission ('TLGC') to investigate the use of facial recognition technology to minimise gambling harm;[269]

[261] Privacy Act Review Report 2022 Proposal 13.2 and 126–127.
[262] Government Response.
[263] Privacy Act Review Report 2022 Proposal 4.10.
[264] Ibid 45.
[265] Ibid 2022 46.
[266] Government Response 6.
[267] Issues Paper Part 2, Question 2.5.
[268] See Tasmania, *Parliamentary Debates*, Legislative Council, 24 August 2021, 27–28.
[269] See Tasmanian Liquor and Gaming Commission, *Investigation of Harm Minimisation Technologies: Facial Recognition and Player Card Gaming* (Report to the Treasurer, June 2022) <https://www.treasury.tas.gov.au/Documents/TLGC%20Report%20to%20Treasurer%20-%20Investigation%20of%20harm%20minimisation%20technologies.PDF>.

- reports of national retailers and operators of stadia collecting patrons' biometric data, either without consent, or where consent is a condition of entry.[270]

4.9.3 The Tasmanian Council of Social Service ('TasCOSS') raised other concerns about biometrics, including the growth of surveillance in public places, use of data in police profiling, and concerns about bias in biometric technologies leading to unjust or discriminatory outcomes.[271]

4.9.4 Dr Sarah Moulds submitted that the use of facial recognition technology ('FRT') 'must be subject to strict safeguards and limitations in order to constitute a justifiable limitation of the right to privacy'. Dr Moulds argued that FRT can be a rights-enhancing tool if certain conditions are met (including assurance of the accuracy of the technology, the security of data, and the security of data storage), if there is informed consent for obtaining, using, and sharing facial images, and if legal safeguards and protections are in place.[272]

4.9.5 Two submissions (the submission of Professor Margaret Otlowski, Emeritus Distinguished Professor Dianne Nicol, and Dr Lisa Eckstein of the Centre for Law and Genetics at the University of Tasmania, and the submission of Meg Webb MLC) argued that the PIPA should be amended to align the definition of 'sensitive information' with that in the Privacy Act by identifying genetic information about an individual that is not otherwise health information as a form of 'sensitive information'.[273]

4.9.6 The Centre for Law and Genetics team further submitted that, if the Privacy Act Review proposals are adopted, the definition of 'sensitive information' should be further amended to replace 'about' with 'relates to' (for the sake of consistency) and to identify genomic information as a form of 'sensitive information'.[274]

4.10 The TLRI's view

4.10.1 The TLRI acknowledges the concerns raised in the submissions about the increased privacy challenges created by developments in technology. In the TLRI's view, it would be appropriate to align the definition of 'sensitive information' in the PIPA with that in the Privacy Act by adding biometric information and genetic information about an individual that is not otherwise health information to the PIPA definition.

4.10.2 The TLRI also recommends that the definition of 'health information' be amended to align with the definition of 'personal information' (see [4.7.6]) for clarity and consistency.

4.10.3 Additional reforms to the PIPA to align with proposals in the Privacy Act Review Report should also be considered, if those proposals are enacted at the Commonwealth level; namely,

- amending the definition of 'sensitive information' to replace 'about' with 'relating to' (to align with the same proposed change to the definition of 'personal information');
- amending the definition of 'sensitive information' to include genomic information;
- amending the definition of 'sensitive information' to include inferences about sensitive information; and

[270] Submission 8 (Meg Webb MLC).
[271] Submission 11 (TasCOSS).
[272] Submission 18 (Dr Sarah Moulds).
[273] Submission 17 (Centre for Law and Genetics); Submission 8 (Meg Webb MLC).
[274] Submission 17 (Centre for Law and Genetics).

- defining geolocation tracking data and specifying that such data can only be collected, used, disclosed, and stored with consent.

4.10.4 The TLRI also notes that the Privacy Act Review discussed concerns that exist in relation to high privacy risk activities involving facial recognition and other biometric technologies. This was identified as a matter for a coordinated approach across government. The TLRI agrees that this is a matter of concern and similarly that a coordinated response both at a State and Commonwealth level should be adopted.

4.11 Recommendations

Recommendation 5: The definition of 'sensitive information' in the PIPA should be amended to include:

- biometric information used for the purpose of automated biometric verification or biometric identification;
- biometric templates; and
- genetic information about an individual that is not otherwise health information.

Recommendation 6: If recommendation 1 is implemented, the definition of 'sensitive information' should also be amended to replace 'about' with 'relating to'.

Recommendation 7: The definition of 'health information' in the PIPA should be amended to align with the definition of 'personal information'.

Recommendation 8: In line with developments at the Commonwealth level and the desirability of consistency with the approach in other jurisdictions, further consideration should be given to amending the PIPA to expand the definition of 'sensitive information' to:

- include genomic information; and
- include inferences about sensitive information.

Recommendation 9: Pending the outcome of the Commonwealth Privacy Act Review, further consideration be given to amending the PIPA to:

- insert a definition of geolocation tracking data; and
- specify that such geolocation tracking data can only be collected, used, disclosed, and stored with consent.

4.12 Information that receives a lower level of protection under the PIPA or other privacy legislation

The Tasmanian position

4.12.1 In Tasmania, some types of information receive less than the general level of legislative privacy protection due to exceptions or exemptions created by the PIPA or other legislation. These are based on either the nature of the information or the context in which the information is used.

4.12.2 This sub-section discusses most instances of partial or complete exemptions from the PIPA. It does not discuss:

- exceptions applying to certain bodies such as courts and tribunals and various public legal officers, which are addressed in Part 3 above; or
- exceptions relating to the handling of information in a way authorised by law, including by other legislation ancillary to the PIPA, which are discussed in Parts 4 and 6, below.

Basic personal information

4.12.3 In the PIPA, 'basic personal information' is defined to mean the name, residential address, postal address, date of birth, and gender of an individual.[275]

4.12.4 Section 12 of the PIPA permits personal information custodians that are public authorities[276] to use or disclose basic personal information for a purpose other than the primary purpose of collection without the individual's consent in a narrow set of circumstances. These are: (1) where the use or disclosure is reasonably necessary for the efficient storage and use of the information; and (2) where the information is only used by, or disclosed to, 'another public sector body'.

Employee information

4.12.5 The PIPA defines 'employee information' non-exhaustively as personal information about an individual relating to their current, past, or prospective employment in relation to a range of matters such as the individual's selection, employment, training, discipline or resignation, their termination, or the terms and conditions of their employment.[277]

4.12.6 While employee information is characterised as a form of personal information,[278] it is accorded distinct treatment under the PIPA in the sense that certain PIPP requirements do not apply to employee information. These include requirements relating to:

- collection—the requirements in PIPP 1(4) and (5) that personal information about an individual be collected from that individual where it is reasonable and practicable, and the requirement

[275] PIPA 3 (definition of 'basic information').
[276] See the definition in Part 3, above.
[277] PIPA s 3 (definition of 'employee information'). According to this definition, 'employee information' also includes: performance or conduct in carrying out their employment functions or duties, suitability for their employment, hours worked, salary, membership of a professional association, trade association or trade union, information supporting statistical reporting or personnel planning, or other information in relation to employees required by law: ibid.
[278] PIPA s 3 (definition of 'employee information').

that the individual be informed of the collection and related matters (discussed further in Part 5, do not apply to employee information;

- use of unique identifiers—the limitations on the assignment, adoption, use, disclosure, or requirement of unique identifiers in PIPP 7 (discussed further in Part 7) do not apply in relation to employee information; and
- sensitive information—to the extent that the employee information includes sensitive information that would otherwise be subject to additional protections under PIPP 10 (discussed further in Part 5), these additional protections do not apply.[279]

4.12.7 Employee information is also treated differently in PIPP 2, which concerns the use and disclosure of personal information. PIPP 2 holds that personal information can generally only be used and disclosed for the purpose for which it was collected (see Part 5), but express exceptions allow other use or disclosure of employee information, if:

- it is to be used to assess a person's suitability for appointment or for employment they already hold;[280] or
- it is being transferred to another personal information custodian for use as employee information.[281]

Public information

4.12.8 The PIPA does not apply to public information,[282] meaning:

> 'any personal information that is:
>
> (a) contained in a publicly available record or publication; or
>
> (b) taken to be public information under any Act'.[283]

Law enforcement information

4.12.9 In the PIPA, personal information custodians that are a law enforcement agency may be exempt from one or more PIPP requirements in certain circumstances. The PIPA definition of 'law enforcement agency' encompasses a range of bodies, including police forces (of the Commonwealth, Tasmania, other States or Territories, and foreign countries), Tasmanian entities responsible for protecting public revenue (for example, levies, taxes, rates, and royalties), and Tasmanian entities responsible for administering or performing functions that impose a penalty or sanction.[284]

4.12.10 Under the PIPA, several obligations or limitations on personal information custodians' information handling under PIPPs 1, 2, 5, 7, 9 and 10 do not apply to 'law enforcement information'

[279] PIPA s 10.
[280] PIPA sch 1, PIPP 2(1)(i).
[281] PIPA sch 1, PIPP 2(1)(j). This might include, for example, allowing someone's past employment record, including union membership, to be shared and maintained by a new employer, or as a record relating to employment at other public authorities.
[282] PIPA s 8.
[283] PIPA s 3.
[284] PIPA s 3 (definition of 'law enforcement agency').

collected or held by one of these law enforcement agencies.[285] These include, among others: the requirement to take reasonable steps to notify an individual of certain details before, during, or after the collection of personal information;[286] the prohibition on use or disclosure of personal information except in the circumstances specified in PIPP 2;[287] and the prohibition on the collection of sensitive information except in the circumstances specified in PIPP 10[288] (which are discussed in detail in Part 5 of this Report).

4.12.11 The law enforcement exemption applies where the law enforcement agency considers that non-compliance with the PIPP is reasonably necessary:

- for the purpose of any of its functions or activities;
- for the enforcement of laws relating to confiscating proceeds of crime; or
- in connection with the conduct of proceedings in any court or tribunal.[289]

4.12.12 Information may also be subject to exceptions where it could be *useful to* law enforcement agencies. PIPP 2 generally requires that personal information be used and disclosed only for the purpose for which it was collected. However, an exception exists where the information custodian reasonably believes that its use and disclosure is reasonably necessary for various purposes by a law enforcement agency or on its behalf.[290]

4.12.13 The term 'law enforcement information' is defined in the PIPA by reference to 'information referred to in s 30 of the Right to Information Act 2009'.[291] That section of the *Right to Information Act 2009* (Tas) ('RTI Act') states that information is law enforcement information, if its disclosure would or would be reasonably likely to:

- prejudice the investigation of a breach or enforcement or proper administration of the law;
- prejudice the fair trial of a person or the impartial adjudication of a particular case;
- disclose or enable a person to ascertain the identify of a confidential source;
- prejudice the effectiveness of methods or procedures relating to breaches of the law;
- endanger a person's life or safety or increase the likelihood of harassment or discrimination of a person;
- disclose information collected for intelligence including criminal databases; or
- hinder, delay or prejudice an investigation of a breach or possible breach of the law which is not yet complete.[292]

4.12.14 Under the RTI Act, the above-listed information will constitute 'law enforcement information' (and so be exempt from disclosure under that Act), even where it reveals unlawful behaviour by law enforcement bodies, such as information that reveals the use of illegal methods to

[285] Namely, the following PIPPs are not applicable to law enforcement information: 1(3), (4) and (5) (relating to collection of personal information); 2(1) (use and disclosure); 5(3)(c) (responding to a request on how a custodian collects, holds, uses, and discloses that information); 7 (unique identifiers); 9 (disclosure outside of Tasmania); and 10(1) (restrictions on collection of sensitive information).
[286] PIPP 1(3).
[287] PIPP 2(1).
[288] PIPP 10(1).
[289] PIPA s 9.
[290] PIPA sch 1, PIPP 2(1)(g).
[291] PIPA s 3 (definition of 'law enforcement information').
[292] *Right to Information Act 2009* (Tas) s 30(1).

investigate a crime, or general information or reporting of a public authority's approach to investigating breaches or enforcing or administering the law, but only if disclosure of the information is contrary to the public interest.[293]

4.12.15 Whether disclosure of information is in the public interest is to be determined by reference to a non-exhaustive list of 25 matters set out in the RTI Act. These include, for example, whether disclosure would enhance scrutiny of government action and whether it would promote or harm the administration of justice.[294]

Public benefit exemptions

4.12.16 A personal information custodian can apply to the Minister for an exemption relating to any or all provisions of the PIPA.[295] An application for exemption must address a range of matters, including specifying the provisions of the PIPA to which the application relates, the information and personal information custodians to which the application relates, the reasons for seeking an exemption, any public benefit involved, and any law, code or other instrument under which it proposes to operate.[296]

4.12.17 The Minister may 'approve an application if satisfied that the public benefit of the exemption outweighs to a substantial degree the public benefit from compliance with the [PIPPs]', with or without conditions.[297] The exemption may be subject to conditions if the Minister considers it appropriate.[298] If the Minister is not satisfied about the balance of public benefit, they may refuse to grant the exemption.[299]

4.12.18 The Minister may also revoke an application, if satisfied that the reasons for granting the exemption no longer apply or that the balance of public benefit no longer substantially weighs in favour of the exemption. The applicant may also themselves request an exemption be revoked.[300] However, these are merely permissive provisions and do not place obligations on the Minister. The PIPA also does not provide for any application process for revocation.

4.12.19 Any determination (whether an approval or a refusal) or revocation must be published in the Gazette.[301] There is no easily accessible list of exemptions currently in operation. An examination of the Gazette suggests there were 11 public benefit exemptions published between 2008 and 2020 as follows: two in April 2011; one in February 2019; and eight in November 2020.[302] As an example, on 25 November 2020, exemptions were gazetted for information relevant to a civil claim against the State of Tasmania that was held by nine government departments.[303]

[293] *Right to Information Act 2009* (Tas) s 30(2).
[294] *Right to Information Act 2009* (Tas) sch 1.
[295] PIPA s 13.
[296] PIPA s 13.
[297] PIPA s 14(1)(a).
[298] PIPA s 14(2).
[299] PIPA s 14(1)(b).
[300] PIPA s 15.
[301] PIPA ss 14(3), 15(2).
[302] The *Tasmanian Government Gazette* is available at <http://www.gazette.tas.gov.au/editions>.
[303] Tasmania, *Gazette*, No 22037, 25 November 2020 <http://www.gazette.tas.gov.au/editions/2020/november_2020/22037_-_Gazette_25_November_2020.pdf>.

Emergency declarations

4.12.20 The PIPA does not provide any general exceptions or exemptions relating to responding to emergency situations.

The position in other jurisdictions

Basic information

4.12.21 No other State and Territory privacy legislation, or the Commonwealth Privacy Act, distinguishes 'basic personal information' from other personal information in order to facilitate use or disclosure between public authorities for the efficient storage and use of the information.[304]

Employee information

4.12.22 Privacy legislation in other States and Territories does not create exemptions in relation to the handling of employee information.

4.12.23 The Commonwealth Privacy Act generally exempts employers' handling of employee records[305] and information relating to the employment relationship from the Act's privacy requirements.[306] This exemption applies to organisations—meaning non-public sector entities—but not to agencies such as Commonwealth Departments and other bodies established under Commonwealth statutes.[307] It only extends to personal information in an employee record that is used or disclosed for a purpose directly related to the employment relationship.[308]

Public information

4.12.24 By not protecting publicly available information, the PIPA operates in a similar way to privacy legislation in some other jurisdictions including NSW,[309] Victoria,[310] Queensland,[311] and the NT.[312]

4.12.25 In contrast, the Commonwealth Privacy Act does not have a general exemption that removes protections for publicly available information.

---

[304] The Privacy Act does define a similar category of 'identification information' as a subset of 'credit information' relating to the credit reporting provisions of the Act: PIPA ss 3 (definition of 'identification information' and 'credit information), 6N. Some other State and Territory legislation makes some special provision for information exchanges between public authorities, or in relation to information sharing under other legislation (see Part 9).
[305] Defined in similar terms to employee information in the PIPA with the addition of taxation, banking, or superannuation affairs: *Privacy Act 1988* (Cth) s 6 (definition of 'employee record').
[306] *Privacy Act 1988* (Cth) s 7B(3).
[307] Privacy Act Review Report 2022, 64; *Privacy Act* s 7B(3).
[308] *'QF' & Others and Spotless Group Limited (Privacy)* [2019] AICmr 20; see Privacy Act Review Report 2022 64.
[309] *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3)(b).
[310] *Privacy and Data Protection Act 2014* (Vic) s 12.
[311] *Information Privacy Act 2009* (Qld) sch 1 cl 7(a).
[312] *Information Act 2002* (NT) s 68.

Law enforcement information

4.12.26 Other jurisdictions, such as NSW, Victoria, Queensland, and the NT prescribe exemptions to requirements under some privacy principle requirements for law enforcement agencies (and, in some cases, other bodies) in relation to law enforcement activities.[313]

4.12.27 The Commonwealth Privacy Act also specifies several exemptions or limitations on the application of the APPs to an 'enforcement body', or to an APP agency[314] or organisation[315] in relation to specified uses or disclosures to an enforcement body or relating to the activities of an enforcement body. For example, elements of the APPs do not apply if collection, use, or disclosure of certain information is reasonably necessary for an 'enforcement body' to carry out its functions.[316] There is also a limit on individuals' right of access to personal information about themselves, where any APP entity suspects unlawful activity or serious misconduct has been, is being, or may be, engaged in, and giving access would prejudice the taking of appropriate action or enforcement by enforcement bodies.[317]

4.12.28 The Privacy Act definition of 'enforcement body' is broad and includes the Australian Federal Police, the Immigration Department, the Office of the Director of Public Prosecutions, Commonwealth and State anti-corruption bodies, and authorities and bodies established to conduct criminal investigations or inquiries under State and Territory law.[318]

4.12.29 Rather than defining 'law enforcement information' or 'enforcement information', the Privacy Act defines 'enforcement related activity' as follows:

> (a) the prevention, detection, investigation, prosecution or punishment of:
> (i) criminal offences; or
> (ii) breaches of a law imposing a penalty or sanction; or
> (b) the conduct of surveillance activities, intelligence gathering activities or monitoring activities; or
> (c) the conduct of protective or custodial activities; or
> (d) the enforcement of laws relating to the confiscation of the proceeds of crime; or
> (e) the protection of the public revenue; or
> (f) the prevention, detection, investigation or remedying of misconduct of a serious nature, or other conduct prescribed by the regulations; or
> (g) the preparation for, or conduct of, proceedings before any court or tribunal, or the implementation of court/tribunal orders.

Public benefit or public interest exemptions

4.12.30 Other Australian jurisdictions, such as NSW, Victoria, and Queensland, provide for similar exemptions on the basis of the public interest to those found in the PIPA. These states, however, give the power to make exemptions to an independent office-holder appointed under the privacy legislation,

---

[313] See, eg, *Privacy and Personal Information Protection Act 1998* (NSW) s 23; *Privacy and Data Protection Act 2014* (Vic) s 15; *Information Privacy Act 2009* (Qld) s 29; *Information Act 2002* (NT) s 70. Note the amendments contained in the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) (yet to commence).
[314] *Privacy Act 1988* (Cth) sch 1, cl 3.4 (collection), cl 6.2 (use and disclosure).
[315] See, eg, *Privacy Act 1988* (Cth) cl 9.2(e), 12.3(h).
[316] *Privacy Act 1988* (Cth) sch 1, cl 3.4, cl 6.2, cl 8.2.
[317] *Privacy Act 1988* (Cth) s 16A, sch 1 cl 12.3(h) and (i).
[318] See, eg, *Privacy Act 1988* (Cth) cl 6.3 (use and disclosure), cl 8.2(f).

such as the Information Commissioner in Victoria[319] and Queensland[320] and the Privacy Commissioner (with the approval of the Minister) in NSW.[321] In Victoria and Queensland, State Parliament also has the power to disallow a public interest exemption.[322]

4.12.31 The Commonwealth Privacy Act also provides for the making of public interest determinations which excuse breaches of privacy, either where they may occur in the future or after they have occurred. Where an entity's acts or practices may breach, or have breached, a privacy obligation, the Australian Information Commissioner (described in Part 2) may make a public interest determination if satisfied that the public interest in the act or practice substantially outweighs the public interest in adhering to the privacy obligation.[323] For as long as the determination is in force, acts or practices that would otherwise contravene privacy obligations are not taken to be breaches of the Privacy Act.[324]

4.12.32 Where an urgent decision is needed, the Privacy Act also allows the Information Commissioner to make a temporary determination,[325] including on the Commissioner's own initiative (without an application).[326] The OAIC maintains a register of public interest determinations.[327] There have been eight declarations since 2015, with five currently in effect.

Emergency declarations

4.12.33 Part VIA of the Privacy Act allows for the Prime Minister or Minister to make an emergency declaration. The declaration has the general effect of overriding otherwise-applicable privacy requirements for the purpose of responding to emergencies or disasters, including allowing all entities subject to the Commonwealth APPs to handle personal information without the consent of the person concerned. An emergency declaration also protects entities against breaches of secrecy provisions in other legislation and obligations of confidence that exist in general law.[328]

4.12.34 Some State and Territory legislation exempts public authorities from privacy compliance in emergency situations. For example, in NSW, public authorities are not required to comply with the information protection principles where the information handling is reasonably necessary to assist in a state of emergency, is only for that purpose, and it is unreasonable or impracticable to obtain the individual's consent.[329] In Queensland, a more limited exemption applies to the collection of personal information in the context of delivery of an emergency service; in that circumstance, agencies are not

[319] *Privacy and Data Protection Act 2014* (Vic) ss 8C(1)(c), 29.
[320] *Information Privacy Act 2009* (Qld) ss 136, 157 (although principles relating to data security and access and correction cannot be disapplied: *Information Privacy Act 2009* (Qld) s 29(3)). Note the amendments contained in the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) (yet to commence).
[321] *Privacy and Personal Information Protection Act 1988* (NSW) s 41.
[322] See, eg, *Privacy and Data Protection Act 2014* (Vic) s 42; *Information Privacy Act 2009* (Qld) s 157(3); *Statutory Instruments Act 1992* (Qld) s 50.
[323] *Privacy Act 1988* (Cth) s 72. The process for the making of applications and determinations is set out in ss 73–79.
[324] *Privacy Act 1988* (Cth) s 80B.
[325] *Privacy Act 1988* (Cth) s 80A.
[326] *Privacy Act 1988* (Cth) s 80A(2).
[327] *Privacy Act 1988* (Cth) s 80E.
[328] *Privacy Act 1988* (Cth) s 80P.
[329] *Privacy and Personal Information Protection Act 1998* (NSW) s 27D. Personal information collected, used, or disclosed under this provision must not be held for longer than 18 months (unless there are extenuating circumstances or consent has been obtained) and law enforcement agencies may not use the information for prosecuting an offence: s 27D(3).

required to take reasonable steps to make individuals aware of the purpose of the collection and related matters.[330] Legislation in other jurisdictions, such as Victoria, is silent on emergency situations.

4.13 The Commonwealth Privacy Act Review

Employee information

4.13.1 The Privacy Act Review reported that submissions calling for removal or narrowing of the employee records exemption applying to non-public sector bodies had expressed concerns about the growing collection of sensitive information associated with public health workplace health and safety requirements, and the growing use of biometric technologies by employers.[331] It also received submissions expressing concern about the removal of the employee records exemption on basis that it would create a compliance burden.[332]

4.13.2 The Review concluded that there was a need for 'recalibration' of this and other exemptions in order to meet community expectations and address privacy risks in the digital age.[333] It proposed the introduction of enhanced privacy protections for employee records of private sector employees. These reforms would:

- enhance transparency to employees in terms of 'what their personal and sensitive information is being collected and used for';
- ensure employers have flexibility to collect, use, and disclose employee information, where reasonably necessary to administer the employment relationship;
- ensure employees' personal information is protected from misuse, loss, or unauthorised access, and that it is destroyed when no longer required; and
- place an obligation on employers to notify employees and the Australian Information Commissioner where there has been a data breach involving an employee's personal information, if the breach 'is likely to result in serious harm' (discussed further at Part 5).[334]

4.13.3 The Review also suggested that further consultation should be undertaken with employer and employee representatives on how the protections should be implemented in legislation, including examining the interaction between privacy and workplace relations laws and the possibility of the development of privacy codes of practice.[335] The Government agreed in-principle with the Review's proposal that further consultation be undertaken.[336]

Public information

4.13.4 The Privacy Act Review did not propose changes to the Privacy Act's application to public information. It did, however, reject suggestions that the Privacy Act could be amended to include a list of information that does *not* constitute personal information (and hence is not subject to the Privacy

[330] *Information Privacy Act* (Qld) sch 3 cl 2(5). It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[331] See Privacy Act Review Report 2022 65.
[332] Privacy Act Review Report 2022 2.
[333] Ibid.
[334] Ibid Proposal 7.1.
[335] Ibid.
[336] Government Response 6.

Act), including publicly available information, arguing that any information specified in such a list 'would not necessarily never be personal information'.[337] The Review suggested that this might discourage APP entities from identifying and addressing privacy issues 'in a flexible, principles-based regime' and drawing on OAIC guidance.[338]

Law enforcement information and public benefit exemptions

4.13.5 The Privacy Act Review made two proposals relevant to exceptions for law enforcement information, one of which also related to public interest exceptions.

4.13.6 The first was a proposal to introduce a law enforcement exception relating to a proposed new right to erasure. The second was a proposal to introduce an exception to the right to erasure and other individual rights proposed by the Review, where complying with a request would be contrary to public interests, including freedom of information and law enforcement activities.[339] These proposals are discussed in detail in Part 6.

Emergency declarations

4.13.7 The Privacy Act Review invited feedback on whether the emergency declaration provisions in Part VIA of the Privacy Act could be improved.[340] The Review proposed amendments to the Privacy Act to:

- enable emergency declarations to be more targeted by entity, classes of personal information or specified acts and practices, on the basis that this would lead to a better balance between sharing individuals' personal information to respond to an emergency and protecting their privacy;[341]
- ensure emergency declarations can be made in relation to ongoing emergencies (such as pandemics) in order to address the apparent limitation of the scope of existing provisions to individuals who are already affected by a disaster;[342] and
- permit organisations to disclose personal information to state and territory authorities—not only to Commonwealth agencies—when an emergency declaration is in place, as long as the State or Territory has enacted comparable privacy laws to the Commonwealth and on the proviso that State and Territory authorities cannot use the information received under an emergency declaration for anything other than a 'permitted purpose' under the Privacy Act.[343] This proposal was intended to better facilitate responses to emergencies and disasters.[344]

4.13.8 The Government agreed with each of these proposals and committed to developing legislative proposals for further targeted consultation.[345]

[337] Privacy Act Review Report 2022 29.
[338] Privacy Act Review Report 2022 29.
[339] Ibid Proposals 18.1, 18.2,
[340] See ibid 47.
[341] Ibid Proposal 5.3, 50.
[342] Ibid Proposal 5.4, 51.
[343] Privacy Act Review Report 2022 Proposal 5.5, 51.
[344] Ibid 51.
[345] Government Response 2, 16.

4.14 Consultation

4.14.1 The TLRI Issues Paper asked the following question regarding information that receives a lower level of protection under Tasmanian privacy legislation:

> Are the exceptions, including the process for declaring and publishing public benefit exemptions, suitable?[346]

4.14.2 Submissions in reply to the Issues Paper focused on the public benefit exemption provisions (discussed above at [4.12.16]–[4.12.19]).

4.14.3 Meg Webb MLC submitted that the current provisions are inadequate and proposed that the PIPA be amended to introduce a requirement for Ministerial determinations to be disallowable by Parliament, as per privacy legislation in Queensland, NSW, and Victoria.[347]

4.14.4 Mr Richard Griggs also criticised the public benefit exemption mechanism. Mr Griggs cited the example of a PIPA exemption gazetted on 25 November 2020, which applies to eight departments in relation to any information that 'has the potential to be relevant to an actual or potential civil claim against the State of Tasmania'. Mr Griggs submitted that the existing exemption process is problematic for several reasons, including: that it 'amounts to government applying to itself to be exempted from legal obligations'; that it does not require the Minister to involve the public or the Tasmanian Ombudsman; and that it does not provide an avenue for members of the public to seek a review of the decision. In regard to the latter, Mr Griggs observed that decisions of the Anti-Discrimination Commissioner to grant an exemption from compliance with the *Anti-Discrimination Act 1998* (Tas) are reviewable.[348] Mr Griggs asserted that:

> it does not appear reasonable or necessary for the government to have a 'back stop' exemption that allows it to simply and easily exempt itself from compliance at its own election.[349]

4.14.5 Mr Griggs recommended that Sections 13 and 14 of the PIPA be repealed altogether, on the basis that other specific exemptions are available elsewhere in the PIPA (namely, those relating to courts and tribunals, public information, law enforcement information, employee information, unsolicited information, and basic information).

4.14.6 Mr Kelvin Markham expressed the view that an exemption should be introduced to permit Marine and Safety Tasmania to publish the names of mooring owners on the Land Information System Tasmania ('LIST') data portal. Mr Markham submitted that the exclusion of this information from public view 'leads to inefficiency in the use of moorings and prevents the ready identification of mooring owners and lessees'. He contrasted this with the availability of searches of property records under the *Land Titles Act 1980* (Tas).[350]

[346] Issues Paper Part 2, Question 2.6.
[347] Submission 8 (Meg Webb MLC).
[348] Submission 10 (Richard Griggs); *Anti-Discrimination Act 1998* (Tas) s 59.
[349] Submission 10 (Richard Griggs).
[350] Submission 2 (Kelvin Markham). The *Land Titles Act 1980* (Tas) provides for the Register of Land Titles (and other associated documents) to be public records.

4.15 The TLRI's view

Basic personal information

4.15.1 The TLRI notes that the basic personal information provision in Section 12 of the PIPA (discussed at [4.12.3] above) is inconsistent with the approach in the Commonwealth and other State and Territory legislation, which do not create a general exemption for use or disclosure of basic personal information between public bodies for storage or usage purposes. No submissions were received in relation to this issue, and it is unclear whether the distinction between basic personal information and personal information has a practical application in Tasmania. However, in light of its recommendation that there should be consistency with other jurisdictions, the TLRI's view is that consideration should be given to aligning the definition of personal information in Tasmania with the approach in the Commonwealth Privacy Act and other jurisdictions.

4.15.2 On this basis, the TLRI considers that the exception relating to the use or disclosure of 'basic personal information' set out in Section 12 of the PIPA should be subject to further targeted consultation on the purpose and utilisation of this provision by public authorities and whether it is necessary in light of other provisions facilitating information sharing between government bodies (discussed in Part 7 of this Report).

Employee information

4.15.3 The TLRI observes that the PIPA is the only privacy statute in Australia that creates information handling exceptions in relation to employee information for public sector bodies. Other State and Territory legislation makes no mention of employee information, while the Privacy Act exception applies only to non-public sector employers at the Commonwealth level.

4.15.4 The TLRI also observes that the Privacy Act Review argued that there is a strong case for narrowing the employee information exception for non-public sector bodies because of the growing range of data held by employers, including sensitive health information and biometric information, and the proliferation of technology available to analyse and utilise that data (including for employment-related purposes). As noted in the Privacy Act Review, the original purpose of the employee information exemption was on the grounds that 'the handling of employee records [was] a matter better dealt with under workplace relations legislation'.[351] However, it was still recognised that personal information about employees was a matter that warranted privacy protection.[352]

4.15.5 Given the increased range of data held by employers, as outlined above, and that Tasmania is the only jurisdiction that exempts employee information held by public sector bodies, the TLRI's view is that the exemption should be removed. However, the TLRI notes it did not receive any submissions that addressed this issue.

Public information

4.15.6 The TLRI considers that the exception relating to public information in the PIPA should be removed in light of:

[351] Privacy Act Review Report 2022 64.
[352] Ibid.

- the inconsistency of the PIPA provision with privacy legislation in other jurisdictions; and
- the Privacy Act Review's proposal that judgments about whether information constitutes personal information should be determined through principles-based assessment by regulated bodies without the imposition of inflexible, blanket exemptions for certain types of information, including public information.

4.15.7 The TLRI is also of the view that the continued exclusion of public information from the definition of 'personal information' in the PIPA would also be inconsistent with the proposed introduction of a right to erasure regarding public information, discussed in Part 6 below.

4.15.8 The TLRI acknowledges that removing the public information exemption may have significant resource implications for Tasmanian public authorities, which should be considered prior to any reform being implemented.

Law enforcement information

4.15.9 Drawing on the Privacy Act Review Report, the TLRI is of the view that changes to the PIPA that create or enhance individual rights relating to personal information (such as a right to erasure and a right to object) would necessitate the creation of exceptions for law enforcement activities. These are addressed in Part 6 below.

4.15.10 Further, the TLRI's view is that there is a lack of clarity in relying on the definition of 'law enforcement information' in Section 30 of the RTI Act and there would be a benefit to having a definition or information in the PIPA that reflects the circumstances in which law enforcement information should be exempt from PIPA requirements. On this basis, the TLRI recommends that a definition of law enforcement information should be included in the PIPA.

Public benefit exemptions

4.15.11 In the TLRI's view, the Ministerial exemption mechanism based on a public benefit assessment in the PIPA should be amended to introduce a mechanism making public interest determinations made by the Minister subject to disallowance by the Parliament. This would align the PIPA with legislation in several other States and Territories and would be consistent with the separation of powers and the principle that Parliament (not the Executive) should control law-making.[353]

4.15.12 In the alternative, as noted at [4.12.30], other jurisdictions provide powers to an independent office-holder appointed under the privacy legislation in relation to the public benefit exemption. Accordingly, the TLRI is of the view that it would be appropriate for the body responsible for broadened enforcement and compliance functions under the PIPA (see Recommendation 47 in Part 8 of this Report) to be empowered to make public interest determinations under the PIPA (aligning with the approach taken by the Commonwealth, Victoria, and Queensland), if this power was checked by the parliamentary disallowance mechanism described above.

4.15.13 If these safeguards are introduced, the TLRI does not consider that a right for the public to seek review of public benefit exemptions is necessary, noting that no such right is established in the Privacy Act or equivalent State and Territory privacy legislation.

[353] Harry Evans and Rosemary Laing (eds), *Odgers' Australian Senate Practice* (14th ed, Department of the Senate, Canberra, 2012) 429, 433.

Emergency declarations

4.15.14 The TLRI notes that several major reviews, including the Royal Commission into National Natural Disaster Arrangements and the Privacy Act Review, identified a need for improvements to information sharing in relation to natural disasters and ongoing emergencies.

4.15.15 The Royal Commission recommended that all Australian governments should ensure that personal information of individuals affected by a natural disaster can be appropriately shared between all levels of government, agencies, insurers, charities, and organisations delivering recovery services. The Royal Commission qualified that this must account for all necessary safeguards to ensure the sharing is only for recovery purposes.[354]

4.15.16 In the Privacy Act Review, it was proposed that amendments to the Commonwealth Privacy Act be made to better facilitate the sharing of information by organisations with State and Territory governments in emergencies would be appropriate.

4.15.17 Similarly, it is the TLRI's view that exemptions for information handling in emergency situations should be provided for in the PIPA.

4.16 Recommendations

Recommendation 10: Section 12 of the PIPA should subject to further consultation with public authorities, to clarify whether the provision is necessary in light of other information-sharing provisions in the PIPA.

Recommendation 11: The employee information exemptions in the PIPA should be removed.

Recommendation 12: The public information exception in the PIPA should be removed. Consideration should be given to ensuring that appropriate resources, guidance and transition periods are set to enable public authorities to comply with this amendment.

Recommendation 13: A definition of 'law enforcement information' should be included in the PIPA.

Recommendation 14: The public benefit exemption mechanism should be amended to either:

(a) introduce a mechanism making Ministerial public benefit determinations subject to disallowance by the Parliament; or
(b) if Recommendation 47 is adopted and an independent office-holder (such as an information commissioner or a privacy commissioner) is established, confer the power to make public benefit determinations on that office-holder, subject to disallowance by the Parliament.

Recommendation 15: There should be appropriate exemptions for information handling in emergency situations in the PIPA.

[354] Australian Government, *The Royal Commission into National Natural Disaster Arrangements Report* (Report, 2020) Recommendation 22.2.

Part 5

Aligning the Personal Information Protection Principles with the Commonwealth Act: Collection, Use, and Disclosure

5.1 Overview of this Part

5.1.1 As discussed in Part 2, reviews of privacy legislation at the Commonwealth level and in multiple States and Territories have called for greater consistency across jurisdictions. Several submissions in response to this project's Issues Paper expressed a similar view that Tasmanian information privacy legislation should be consistent with other jurisdictions; the TLRI's view is that consistency is a desirable goal (see [2.8]).[355] This includes consistency between the Personal Information Protection Principles ('PIPPs') established in Tasmania's PIPPs and similar principles in other legislation, especially the Australian Privacy Principles ('APPs').

5.1.2 The *Personal Information Protection Act 2004 (Tas)* ('PIPA') was intended to enact Tasmanian privacy principles that were broadly consistent with those in the Commonwealth *Privacy Act 1988* (Cth) ('Privacy Act').[356] There have since been amendments to, and reviews of, the Commonwealth legislation. This Part, and Parts 6–8 below, consider and compare those developments with the Tasmanian position to identify areas of inconsistency and options for reform.

5.1.3 The PIPA establishes 10 PIPPs and obliges 'personal information custodians' (bodies subject to the PIPPs: see Part 3) to comply with them.[357] The PIPPs address:

1. the collection of personal information;
2. the use and disclosure of personal information;
3. the quality of personal information;
4. safeguarding personal information from misuse, loss, unauthorised access, modification or disclosure;
5. openness through policies on the handling of personal information;
6. access and correction of individuals' personal information;

[355] Submission 3 (Anonymous); Submission 8 (Meg Webb MLC); Submission 12 (Youth Law Australia); Submission 17 (Centre for Law and Genetics).
[356] *Personal Information Protection Bill 2004*, Second Reading Speech (Mrs Jackson, 20 October 2004, pt 2, 29–106): 'The personal information protection principles are consistent with the national privacy principles implemented by the Commonwealth in 2001 to amend the Privacy Act to extend the application of the legislation to the private sector'.
[357] PIPA s 17(1).

7. the assignment of unique identifiers to individuals;
8. the option of anonymity for individuals when transacting with personal information custodians;
9. disclosure of personal information to bodies outside of Tasmania; and
10. the collection of sensitive information, such as information on race, ethnicity, or criminal history.

5.1.4 This Part, and Parts 6–8, consider the similarities and differences between each of the PIPPs and the Commonwealth APPs (as they apply to government agencies) and whether reform is necessary, based on consistency arguments and other considerations identified in research and/or submissions. Recent and proposed amendments to data privacy legislation in some Australian jurisdictions have also drawn heavily on the European Union's *General Data Protection Regulation 2016/679* ('GDPR'); the relevant GDPR provisions are discussed in this Part, where relevant.

5.1.5 The PIPA (in PIPPS 1, 2, 9 and 10) and equivalent legislation in other States and Territories, and at the Commonwealth level, places a range of limitations and obligations on regulated entities in relation to their handling (collection, use, and disclosure) of personal information about individuals. This Part focuses on those provisions.

5.2 The Tasmanian position

Collection of personal information

5.2.1 Under Tasmanian law, PIPP 1 restricts the collection of personal information to circumstances where collection is 'necessary for one or more of … [the custodian's] functions or activities'. The PIPA does not specify how a custodian's functions or activities are determined for the purposes of PIPP 1. Collection is only permitted where it is 'by lawful means'—a term not defined in the PIPA

5.2.2 Individuals must be notified when their information is collected. PIPP 1(3) obliges a personal information custodian to take 'any reasonable steps necessary' to notify the individual—either before collection, during collection, or as soon as practicable after collection—of the personal information custodian's identity and contact information, the individual's right to access to the information, the purpose of information collection, the intended recipients or class of recipients, any laws requiring the information to be collected, and the main consequences to the individual if all or part of the information is not provided.[358] This requirement does not apply to certain law enforcement information collected or held by a law enforcement agency (see [4.12.10]).[359]

5.2.3 PIPP 1(4) requires a personal information custodian to collect information about an individual from that person, if it is reasonable and practicable to do so. This provision does not apply to employee information (defined at [4.12.5]).[360]

5.2.4 According to PIPP 1(5), if personal information about an individual is collected from someone other than the individual, a personal information custodian must take reasonable steps to notify the

[358] PIPA sch 1, PIPP1(3).
[359] PIPA s 9.
[360] PIPA s 10.

individual that their information has been collected, unless this would seriously threaten any individual's life, safety, health, or welfare.[361] This provision does not apply to employee information.[362]

5.2.5 The requirements in PIPP 1(3), (4) and (5) do not apply to certain law enforcement information collected or held by a law enforcement agency (see [4.12.10]).[363]

Collection of sensitive information (including health information)

5.2.6 PIPP 10 places more onerous restrictions on the collection of sensitive information, including health information (see the definition at [4.7.2] above).[364]

5.2.7 Under PIPP 10(1), sensitive information can only be collected where one of the following conditions is met:

- the individual concerned has consented;
- the collection is required or permitted by law;
- the collection is necessary to lessen or prevent a serious or imminent threat to the life or health of any individual and the individual to whom the information relates cannot consent, communicate consent, or is subject to a guardianship or mental health order;
- the information is collected in the course of the activities of a non-profit personal information custodian that has only racial, ethnic, political, religious, philosophical, professional, trade or trade union aims, where the information relates solely to the members of the custodian or individuals who have regular contact with it in connection to its activities and the custodian has undertaken not to disclose that information without consent;
- the collection is necessary for a legal or equitable claim; or
- one of the below exceptions relating to research, provision of services or health information applies.

5.2.8 The exceptions to the requirements in PIPP 10(1) permit the collection of sensitive information about an individual in certain circumstances. First, under PIPP 10(2), a personal information custodian can collect sensitive information about an individual, if the collection is necessary for research or statistical analysis in the public interest and any resulting publication is de-identified, or if the information relates to an individual's racial or ethnic origin and is collected for the purpose of welfare or educational services funded by the government. Such collection is only permitted where there is no practical alternative to collecting the information for these purposes and it is impracticable to seek the individual's consent.

5.2.9 Second, there are three additional circumstances in which health information, as a type of sensitive information, can be collected in the absence of one of the PIPP 10(1) conditions listed at [5.2.7] above. These are:

- under PIPP 10(3), where the information is necessary to provide a health service to the individual concerned, and the information is collected as required by law or in accordance with professional obligations of confidentiality;[365]

[361] PIPA sch 1, PIPP 1(4)–(5).
[362] PIPA s 10.
[363] PIPA s 9.
[364] PIPA sch 1, PIPP 10.
[365] PIPA sch 1, PIPP 10(3).

- under PIPP 10(4) and (5), where the collection is necessary for research or statistical analysis on public health or safety or running a health service, requires information which identifies the individual, it is impractical to seek consent, and the information is collected as required by law or in accordance with professional obligations of confidentiality (in which case, the custodian must take reasonable steps to permanently de-identify the information prior to disclosure);[366] or
- under PIPP 10(6), where the health information is collected from another person and the collection is necessary to provide a health service to that other person and the information is relevant to their social or family history.[367]

5.2.10 The PIPP requirements relating to sensitive information do not apply to law enforcement information collected or held by a law enforcement agency, if it is considered that non-compliance is reasonably necessary for the purpose of any of its functions or activities, enforcement of proceeds of crime laws, or in connection with court or tribunal proceedings (see [4.12.11] above).[368]

Collection of unsolicited information

5.2.11 The PIPA specifies that PIPP 1 does not apply to 'unsolicited information' received by a personal information custodian.[369] The PIPA does not define unsolicited information.

Use and disclosure of personal information (including sensitive information)

5.2.12 PIPP 2 also limits the use and disclosure of personal information. Generally, personal information must only be used or disclosed for the purpose for which it was collected (referred to in this Report as 'the primary purpose').

5.2.13 Personal information can also be used or disclosed for another purpose (referred to herein as 'a secondary purpose'), if it satisfies one of the other circumstances listed in PIPP 2(1).[370] These include circumstances where one of the following conditions is met:

- the purpose of the use or disclosure is related to the primary purpose (and, if it is sensitive information, that information is directly related to the primary purpose) and the individual would reasonably expect use or disclosure for that purpose;
- the individual has consented;
- it is either impracticable to seek prior consent or the recipient is reasonably believed to be not likely to disclose the information, and the use or disclosure is necessary for research or statistical analysis in the public interest (other than for publication in a form that identifies any particular individual);
- the custodian reasonably believes the use or disclosure is necessary to lessen or prevent a serious threat to life, health, safety, or welfare or a serious threat to public health or public safety;
- the use or disclosure is a necessary part of an investigation by the custodian or report to relevant authorities of suspected unlawful activity;

[366] PIPA sch 1, PIPP 10(4), 10(5).
[367] PIPA sch 1, PIPP 10(6).
[368] PIPA s 9.
[369] PIPA s 11.
[370] The terms 'primary purpose' and 'secondary purpose' do not expressly appear in the PIPA and, for the purposes of this discussion, are adopted from APP 6.1 under the *Privacy Act 1988* (Cth).

- the use or disclosure is required or authorised by or under law;
- the custodian reasonably believes the use or disclosure is reasonably necessary for various purposes on behalf of a law enforcement agency, including prevention of crime or breaches of the law, protection of the public revenue, seriously improper conduct, court or tribunal proceedings, investigations into missing persons or matter under the Coroners Act;
- the disclosure has been requested by a Commonwealth security agency; or
- the information is to be used as employee information or transferred to another custodian for such use.[371]

5.2.14 The PIPA creates a further general exception to these restrictions on use and disclosure for law enforcement information collected or held by a law enforcement agency, if it considers non-compliance reasonably necessary for the purpose of any of its functions or activities, enforcement of proceeds of crime laws, or in connection with court or tribunal proceedings (see Part 4).[372]

5.2.15 As discussed at [4.12.3]–[4.12.4], the PIPA establishes that personal information can also be used or disclosed for a secondary purpose where it is 'basic personal information'; in that circumstance, public authorities can share the information with another public sector body where this 'is reasonably necessary for the efficient storage and use of that information'.[373]

5.2.16 PIPP 2(4) also makes explicit provision for health service providers to disclose an individual's health information to another person who is responsible for that individual, where certain conditions are met.[374] These are: the individual is incapable of giving consent or communicating consent; the disclosure is necessary to provide appropriate care or treatment, or is made for compassionate reasons; and the disclosure is not contrary to the wishes of the individual.

5.2.17 The PIPA does not impose specific obligations relating to the use and disclosure of personal information for direct marketing.

Cross-border disclosure

5.2.18 Further restrictions apply to the disclosure of personal information to anyone outside Tasmania. Under PIPP 9, such disclosure is not permitted unless one of the following applies:

- the custodian reasonably believes that the recipient is subject to binding principles substantially similar to the PIPPs;
- the individual concerned consents;
- the disclosure is necessary for the performance of a contract with the individual or for the conclusion or performance of a contract in the individual's interest;
- the custodian has taken reasonable steps to ensure the recipient will not handle the information inconsistently with the PIPPs; or
- the disclosure is authorised or required by any other law.

[371] PIPA sch 1, PIPP 2(1).
[372] PIPA s 9.
[373] PIPA s 12.
[374] PIPP 2(5) sets out when a person is responsible for another.

5.2.19 These restrictions do not apply to law enforcement information collected or held by a law enforcement agency, if it considers it reasonably necessary for the purpose of any of its functions or activities, for enforcing proceeds of crime law or in connection with court or tribunal proceedings (see [4.12.11]).[375]

Consent to collection, use or disclosure

5.2.20 As outlined above, some of the restrictions on the collection, use or disclosure of personal information will not apply to personal information custodians, if the individual about whom the information relates has consented to the information handling. For example, where the individual has consented, a personal information custodian may:

- collect sensitive information;[376]
- use or disclose personal information for a purpose other than the purpose for which it was collected;[377]
- disclose personal information to a person or body outside Tasmania.[378]

5.2.21 Consent is not defined in the PIPA and there are no specific provisions referring to consent of children, or of adults deemed to lack capacity to give consent, with the exception of PIPP 2(4) which permits disclosure of a person's health information to another where the person is 'physically or legally incapable of giving consent' or 'physically unable to communicate consent' to the disclosure.[379]

5.3 The position in other jurisdictions

Collection of personal information

5.3.1 Unlike the PIPA, the Commonwealth Privacy Act contains a definition of 'collects'. It states:

> An entity **collects** personal information only if the entity collects the personal information for inclusion in a record or generally available publication.[380]

5.3.2 This definition of 'collect' is reflected in the wording of the Queensland legislation.[381]

5.3.3 In the Privacy Act, APP 3 governs the collection of solicited personal information. It holds that government agencies and associated bodies[382] must not collect personal information except in one of two scenarios.

[375] PIPA s 9.
[376] PIPP 10(1)(a).
[377] PIPP 2(1)(b).
[378] PIPP 9(b).
[379] PIPP 2(4)(a).
[380] *Privacy Act 1988* (Cth) s 6, emphasis in original.
[381] *Information Privacy Act 2009* (Qld) sch 3 IPP 1. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[382] See the definition of 'agency' in *Privacy Act 1988* (Cth) s 6.

5.3.4 The first is where the collection is reasonably necessary for one or more of the agency's functions. This differs from PIPP 1 in two key respects:

- PIPP 1 permits collection where it is necessary *per se*, while APP 3 permits collection where it is *reasonably* necessary. 'Reasonably necessary' is also a requirement under the legislation in New South Wales ('NSW') and the ACT.[383]
- PIPP 1 mandates collection by lawful means, while APP 3 requires that collection be by lawful and *fair* means. This is also the approach in Victoria and the Northern Territory.[384] The latter approach may preclude intimidation, deception, or unreasonably intrusive measures—even if they are technically lawful.[385]

5.3.5 The second scenario in which government agencies and related bodies can collect personal information under the APPs is where the information is *directly related to* one or more of the agency's functions.[386] The collection of personal information must similarly be directly related to a function of the public sector agency in NSW and Queensland.[387] Guidance from the Office of the Australian Information Commissioner ('OAIC') on APP 3 notes that such functions are identified through reference to the legal instruments which confer or describe the agency's functions.[388] According to the OAIC, 'the activities of an agency will be related to its functions' and can include incidental and support activities, such as human resources and public relations activities.[389]

5.3.6 APP entities that are (private) organisations[390] are more restricted than agencies: they can only collect personal information where it is reasonably necessary for one or more of their functions are activities.[391]

5.3.7 APP 5 imposes a similar notification of collection requirement to the requirement in PIPP 1. It requires that reasonable steps (if any) must be taken to give notice of the collection of personal information at or before the time of collection or, if that is not practicable, as soon as is practicable after collection.[392] This is also the approach in other jurisdictions.[393]

---

[383] *Privacy and Personal Information Protection Act 1998 (*NSW) s 8; *Information Privacy Act 2014* (ACT) TPP 3.
[384] *Privacy and Data Protection Act 2014* (Vic) sch 1, 1.2; *Information Act 2002* (NT) sch 2, 1.2.
[385] See OAIC, *Australian Privacy Principles Guidelines* (Guidance Document, July 2019) ch 3 [3.62]. In the ACT, the information must be either reasonably necessary for, or directly related to, a function or activity of the agency: *Information Privacy Act 2014* (ACT) sch 1 TPP 3.
[386] See OAIC, *Australian Privacy Principles Guidelines* ch 3 [3.62].
[387] *Privacy and Personal Information Protection Act 1998* (NSW) s 8; *Information Privacy Act 2009* (Qld) sch 3 IPP 1. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[388] Ibid [3.10]–[3.12]. 'Legal instruments' are not limited to legislation, but also extends to executive schemes or arrangements.
[389] Ibid [3.11].
[390] See the definition in the *Privacy Act 1988* (Cth) s 6C.
[391] *Privacy Act 1988* (Cth) sch 1, APP 3.2.
[392] *Privacy Act 1988* (Cth) sch 1, cl 5.2.
[393] See *Privacy and Personal Information Protection Act 1998 (*NSW) s 10; *Privacy and Data Protection Act 2014* (Vic) sch 1, 1.3; *Information Act 2002* (NT) sch 2 1.3; *Information Privacy Act 2009* (Qld) IPP 2. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.

5.3.8 Unlike PIPP 1, APP 5 requires entities to disclose who else may have access to the information once it is collected, including overseas recipients, and to disclose that their privacy policy contains information about how to complain about a breach of the privacy principles.[394]

5.3.9 Much like PIPP 1, APP 3 requires information to be collected from the individual, unless it is unreasonable or impracticable to do so.[395] APP 3 provides two additional situations where a public agency may collect information about an individual from someone else, regardless of whether collection from the individual is reasonable or practicable: where the individual concerned has consented, or where the entity is required by law to do so.[396] Unlike the PIPA, the Privacy Act does not create a general exception to collection requirements in relation to law enforcement information collected by law enforcement agencies,[397] except for sensitive information (described below).

Collection of sensitive information (including health information)

5.3.10 Like PIPP 10, APP 3 in the Privacy Act prohibits the collection of sensitive information except in specified circumstances, including where the individual consents, where collection is required or permitted by law and where collection is necessary in relation to a serious or imminent threat, among others.[398] These restrictions do not apply to APP entities that are enforcement bodies (see [4.12.11]), where the entity reasonably believes collection is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.[399]

5.3.11 There are some differences between PIPP 10 and APP 3 in the nature of exceptions to the general prohibition on the collection of sensitive information. Notably, APP 3 permits sensitive information to be collected for the purpose of a confidential alternative dispute resolution process.[400] No equivalent exception appears in the PIPA's principles.

5.3.12 The Privacy Act contains exceptions to the APPs relating to the provision of a health service which are broadly similar to those found in PIPP 10. At the Commonwealth level, the rules apply to sensitive information collected by APP entities that are organisations; that is, private bodies (see [3.2.8] for an explanation of the distinction between organisations and agencies). Collection by agencies is not addressed in the Act, because the Act only applies to private sector health service providers and not to State and Territory public health service providers.[401]

---

[394] *Privacy Act 1988* (Cth) sch 1, cl 5.2. The Privacy Act requirements relating to privacy policies are discussed in Part 7 below.
[395] This is also the approach in Victoria, the Northern Territory, and the ACT.
[396] *Privacy Act 1988* (Cth) sch 1, cl 3.6. Personal information can be collected from someone else with consent in NSW, and the ACT. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[397] Although see the narrower 'permitted general exception' relating to personal information or identifiers where 'the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in' and 'the entity reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter': *Privacy Act 1988* (Cth) s 16 A item 2.
[398] Broadly similar provisions exist in Victoria (sch 1 cl 10), the ACT (sch 1 TPP 3); NT (sch 2 IPP 10); NSW Division 3. In Queensland, health agencies must comply with the NPP (s 31).
[399] APP 3.4. The exception is narrower where the APP entity is the Immigration Department, which must reasonably believe the collection is reasonably necessary for, or directly related to, one or more enforcement or related activities conducted by, or on behalf of, the entity: *Privacy Act 1988* (Cth) s 3.4(d).
[400] See ibid s 16A, sch 1 pt 2 APP 3.
[401] See the brief discussion in Privacy Act Review Report 2022 302.

5.3.13 The Privacy Act permits organisations to collect health information without consent in 'permitted health situations', meaning:

- where the information is necessary to provide a health service, and either the collection is required or authorised under Australian law, or the collection is in accordance with rules of competent health or medical bodies that deal with obligations of professional confidentiality;[402] and
- where the information is about a third party and is part of 'the family, social or medical history' of a patient, where the collection of that history is necessary for the organisation to provide a health service to the patient and it is collected either from the patient or (if the patient cannot give the information) a responsible person.[403]

5.3.14 The Privacy Act also permits both agencies and organisations to collect health information without consent for research purposes. Agencies may act in a manner that would otherwise breach an APP, if it is in the course of medical research and in accordance with privacy guidelines issued by the Chief Executive Officer ('CEO') of the National Health and Medical Research Council ('NHMRC') with approval of the Information Commissioner.[404] By contrast, organisations may collect health information about an individual without consent if:

- the information is necessary for research or the compilation or analysis of statistics relevant to public health or public safety, or the management, funding or monitoring of a health service;
- the purpose cannot be served by collection of de-identified information;
- it is impracticable to obtain the individual's consent; and
- the collection is either required by or under law (other than the Privacy Act), is in accordance with rules established by a competent health or medical body, or is collected in accordance with guidelines issued by the NHMRC CEO or a prescribed authority.[405]

Collection of unsolicited information

5.3.15 In the Privacy Act, APP 4 addresses circumstances where an entity receives personal information that it did not request. In this situation, the entity must determine within a reasonable period whether it *could have* collected the information under APP 3.[406] If the entity would not have been permitted to collect the information, then the information must be destroyed or de-identified as soon as practicable, but only if it is lawful and reasonable to do so.[407] If the collection of the information is permissible, then the other APPs will apply, including obligations to notify the individual concerned.[408]

[402] *Privacy Act 1988* (Cth) s 16B(1).
[403] *Privacy Act 1988* (Cth) s 16B(1A).
[404] *Privacy Act 1988* (Cth) s 95(4).
[405] *Privacy Act 1988* (Cth) ss 16B(2), 95A.
[406] Provisions in relation to unsolicited information also exist in the ACT (TPP 4). It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[407] APP 4.3.
[408] APP 4.4.

Use and disclosure of personal information (including sensitive information)

5.3.16 Under Commonwealth law, APP 6 generally restricts the use or disclosure of personal information to circumstances where such use or disclosure is for the primary purpose for which it was collected.[409]

5.3.17 APP 6 creates a range of exceptions whereby personal information can be used or disclosed for a secondary purpose. Many are similar to those found in the PIPA and the equivalent privacy principles in other jurisdictions.[410] These include:

- use or disclosure to which the individual has consented;[411]
- use or disclosure for a secondary purpose 'related' to the primary purpose (or 'directly related' to the primary purpose, if it is sensitive information), where the individual would reasonably expect use or disclosure for the secondary purpose;
- use or disclosure where required or authorised by or under Australian law or a court or tribunal order; and
- use or disclosure to enforcement bodies where the holder reasonably believes that it is reasonably necessary for enforcement related activities.[412]

5.3.18 Some circumstances identified in the Privacy Act do not have equivalents in the PIPA, or vice versa. For example, the Privacy Act specifies that personal information can be collected, used, or disclosed for a secondary purpose where disclosure is reasonably necessary for a confidential alternative dispute resolution process (see also [5.3.11] above).[413] The Privacy Act does not create an exception for the use or disclosure of employee information to assess an individual's suitability for employment (although organisations are presently exempt from the Privacy Act in relation to employee records: see the discussion in [4.12.23] above).

5.3.19 The Privacy Act, like the PIPA, permits the disclosure of certain information in relation to health and research. First, the Privacy Act permits disclosure of health information about an individual to whom the disclosing organisation is providing a health service, where the recipient of the information is a responsible person for the individual. In this situation, disclosure can be made for a secondary purpose and without the individual's consent. This only applies where the individual is 'physically or legally incapable of giving consent' or 'physically cannot communicate consent', where a person involved in providing the health service is satisfied that the disclosure is necessary, or for compassionate reasons, where the disclosure is not contrary to any expressed or known wish of the individual, and where the disclosure is limited to the extent reasonable and necessary.[414]

5.3.20 The Privacy Act also permits the use or disclosure of health information by organisations for a secondary purpose and without consent, if:

---

[409] APP 6.1.
[410] See PPIP Act (NSW) ss 17-19; Division 3; PDP Act (Vic) sch 1 cl 2; IP Act (Qld) sch 3 IPP 10; IP Act (ACT) sch 1 TPP 6; Information Acy 2002 (NT) IPP2. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[411] APP 6.1(a).
[412] APP 6.1(b), 6.2.
[413] *Privacy Act 1988* (Cth) s 16A. Commonwealth law also permits agencies to use and disclose information for diplomatic or consular functions or activities and allows the Defence Force to use and disclose information for various activities outside Australia such as war or warlike operations, peacekeeping or peace enforcement or civil aid, humanitarian assistance, medical or civil emergency, or disaster relief: ibid.
[414] *Privacy Act 1988* (Cth) s 16B(5); APP 6.2(d).

- it is necessary for research or related purposes relevant to public health or safety;
- obtaining consent would be impracticable;
- the use or disclosure is conducted in accordance with guidelines made under the Act; and
- the discloser reasonably believes the recipient of the information will not disclose it or personal information derived from it.[415]

5.3.21 This is narrower than the equivalent PIPA provision, which permits the use and disclosure of personal information for a secondary purpose where that purpose is research and statistical analysis in the public interest generally (see [5.2.13] above); the Commonwealth law instead makes special provision for the use and disclosure of health information for research or analysis relevant to public health or safety. Exemptions in relation to research also exist in other jurisdictions.[416]

5.3.22 The Privacy Act creates additional avenues for the use and disclosure of several types of information that are not provided for in the PIPA. These are:

- biometric information or biometric templates, which can be disclosed by government agencies and associated bodies (other than an enforcement body) to an enforcement body, if the disclosure is in accordance with guidelines issued by the Information Commissioner;[417] and
- genetic information, which can be used or disclosed by a private organisation in accordance with guidelines made under the Privacy Act if the organisation reasonably believes the use or disclosure is necessary to lessen or prevent serious threat to the life, health, or safety of a genetic relative of the individual.[418]

5.3.23 The Privacy Act also deals with use or disclosure for one purpose not addressed in the PIPA: direct marketing; that is, marketing that involves targeting and communicating with individual consumers directly, such as through telemarketing or mail. Direct marketing is contrasted with marketing undertaken through third parties, such as through advertising media on TV or webpages.

5.3.24 In the Privacy Act, APP 7 imposes obligations on organisations in relation to direct marketing. It does not apply to government agencies, except in limited circumstances where they are engaging in commercial activities.[419] Generally, APP 7 restricts use of personal information for direct marketing, unless the individual has consented to that use. Non-sensitive information which has been collected by the organisation from the individual concerned can also be used for direct marketing, where the individual would reasonably expect their information to be used for that purpose. However, the organisation must provide a simple means to unsubscribe from the marketing.

5.3.25 There is also an exception (under APP 7.1) for contracted service providers to use personal information for direct marketing purposes, where the purpose for which the information was collected,

[415] *Privacy Act 1988* (Cth) s 16B(3); APP 6.2(d).
[416] See, eg, PPIP Act s 27B; PDP Act (Vic) sch 1 Cl 2, 10; IP Act (Qld) IPP 11; *Information Act 2002* (NT) IPP 2. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[417] APP 6.3. As discussed at [4.7.14], certain biometric information and biometric templates are defined as forms of 'sensitive information' in the Privacy Act.
[418] *Privacy Act 1988* (Cth) s 16B(4). As discussed at [4.7.14], genetic information that is not otherwise health information is defined as a form of 'sensitive information' in the Privacy Act.
[419] Note that s 7A of the *Privacy Act 1988* (Cth) provides for government agencies to act as non-government organisations where they are prescribed for this purpose or they are exempted from the *Freedom of Information Act 1982* (Cth) in relation to commercial activities.

and use or disclosure of the information is required to meet an obligation under a Commonwealth contract.

Cross-border disclosure

5.3.26 Under Commonwealth law, APP 8 governs cross-border disclosure of personal information, meaning disclosure to a person 'who is not in Australia or an external Territory'. This scope differs from the equivalent PIPP, PIPP 9, which deals with disclosure outside Tasmania (see [5.2.18] above).[420]

5.3.27 APP 8 is structured differently to PIPP 9 but imposes similar requirements. APP 8 obliges APP entities to 'take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach' the APPs in relation to the information, unless one of a number of exceptions applies.

5.3.28 The Commonwealth and Tasmanian Acts differ in terms of who retains responsibility for breaches of privacy principles by cross-border recipients. According to the OAIC, an entity retains responsibility under the Privacy Act unless one of the exceptions in APP 8.2 applies,[421] whereas the phrasing of PIPP 9 suggests that a personal information custodian is no longer responsible after reasonable steps have been taken.

5.3.29 The exceptions to the 'reasonable steps' requirement in APP 8.2 are also similar to the circumstances of permitted cross-border disclosure in PIPP 9 (by, for example, creating an exception relating to enforcement-related activities),[422] although APP 8 is more restrictive than PIPP 9 in some ways. For example:

- Both PIPP 9 and APP 8 allow disclosure (without reasonable steps), where there is a reasonable belief that the recipient is subject to privacy protection obligations substantially similar to the PIPPs or APPs respectively. However, APP 8 additionally requires that the entity reasonably believes that there are mechanisms for the individual to enforce that protection.
- Both PIPP 9 and APP 8 allow disclosure (without reasonable steps) where an individual has consented to disclosure. However, APP 8 additionally provides that the custodian disclosing the information must expressly inform the individual that, if the individual consents, the custodian is not obliged to take reasonable steps to ensure the overseas recipient does not breach the APPs.[423]
- PIPP 9 permits disclosure outside Tasmania for the purpose of performance of a contract between the individual and the personal information custodian, or for the conclusion or performance of a contract between the custodian and a third party concluded in the individual's interests. APP 8 does not contain a specific exception relating to performance of a contract.[424]

5.3.30 On the other hand, some of the permitted disclosure circumstances in APP 8.2 are broader than those found in PIPP 9. In particular, APP 8 specifies that an agency can disclose information to an overseas recipient in specified 'permitted general situations', such as where there is a reasonable belief

[420] It is noted that in Queensland (IP Act s 33) and the ACT (IP Act TPP 8) provide from the transfer of personal information outside Australia.
[421] *Privacy Act 1988* (Cth) s 16C; see OAIC, *Australian Privacy Principles Guidelines* (2022) [8.2]–[8.3], [8.16]–[8.55].
[422] APP 8.2(f).
[423] APP 8.2(b).
[424] Though there is allowance for authorisation under an international agreement relating to information sharing: see ibid sch 1, APP 8(2)(e)).

that use or disclosure is necessary in relation to a serious risk to life, health, safety, or public health and safety and it would be unreasonable or impracticable to obtain an individual's consent.[425]

Consent to collection, use, or disclosure

5.3.31 As outlined in the preceding sub-sections, some limitations on APP entities' ability to handle certain information will not apply, if the individual who is the subject of the personal information consents to its collection, use, or disclosure. For example, an individual may consent to the collection of information about them from someone else,[426] the collection of sensitive information,[427] the use or disclosure of personal information for a secondary purpose,[428] the use or disclosure of certain personal information for direct marketing,[429] and disclosure of personal information overseas.[430] Legislation in other jurisdictions also provides for consent to be provided that allows for information from another person and also for the use or disclosure of personal information with consent.[431]

5.3.32 Consent is defined in the Privacy Act to mean 'express consent or implied consent'.[432] According to the APP Guidelines issued by the OAIC, the conditions of valid consent are that:

- the individual has sufficient capacity and information to understand the nature of what they are being asked to consent to;
- the individual gives consent voluntarily; and
- the individual gives consent that is current (related to the time of collection, or a specified period thereafter) and specific (not broader than is necessary for its purposes).[433]

5.4 The Commonwealth Privacy Act Review

Collection of personal information

5.4.1 The Privacy Act Review Final Report proposed an amendment to the definition of 'collects' in the Privacy Act to clarify that collection encompasses 'information obtained from any source and by any means, including inferred or generated information', and hence that obligations under APPs 3, 4 and 5 apply to such information.[434] The Commonwealth Government agreed in-principle with this proposal.[435]

[425] For example, where it is necessary to prevent a serious threat to health and safety, to respond to suspected unlawful activity or misconduct, to locate missing persons, or it is related to a legal claim or confidential alternative dispute resolution process: *Privacy Act 1988* (Cth) s 16A.
[426] APP 3.6.
[427] APP 3.3(a).
[428] APP 6.1(a).
[429] APP 7.3(b).
[430] APP 8.2(b).
[431] See, eg, PPIP Act (NSW) s 9, 17(a); PDP (Vic) IPP 2, 9, 10; IP Act (Qld) IPP 10, 11, 33 (note that, in Queensland, agreed/agreement is used rather than consent; IP Act (ACT) TPP 3, 6, 8; Information Act (NT) IPP 2, 79, 10. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[432] *Privacy Act 1988* (Cth) s 6(1).
[433] OAIC, *Australian Privacy Principles Guidelines* ch B, [B.48]–[B.51].
[434] Privacy Act Review Report 2022 Proposal 4.3 and 30.
[435] Government Response 5.

5.4.2 The Review described the purpose of this proposal as being to clarify that the APPs begin to have effect in relation to inferred personal information from the point data is generated (for instance, in data analytics and machine learning processes) and, by extension, to enhance trust in entities using these techniques and clarify that 'reasonable steps to give notice apply where personal information is inferred from unidentified information, such as when actively inferring identity from data about geolocation'.[436] The Review explained that it would mean, for example, that the APPs applied 'where personal information is inferred from unidentified information, such as when actively inferring identity from data about geolocation'.[437] The Review observed that it received comparatively less engagement from stakeholders on this proposal than others.

5.4.3 The Privacy Act Review recommended a number of changes to how individuals are notified of the collection of personal information. First, it proposed that APP 5 be amended to include a requirement for collection notices to be 'clear, up-to-date, concise and understandable', that appropriate accessibility measures be in place,[438] and that collection notices and privacy policies be clear and understandable, particularly for information addressed to a child.[439]

5.4.4 Second, the Review recommended that four additional items be included in the list of matters that must be in an APP 5 collection notice:

- the circumstances of the collection, use, or disclosure if the entity collects, uses or discloses personal information for a high risk activity
- notification to the individual about their rights and how to exercise them;
- that the APP privacy policy (required under APP 1 and discussed in [7.2] of this Report) contains details about how to exercise any rights of the individual (such as the right to object and the other individual rights proposed by the Review, which are discussed further at paragraph [5.4.23] below and Part 6 of this Report); and
- the types of personal information that may be disclosed to overseas recipients (when specifying the countries in which recipients are likely to be located if practicable).[440]

5.4.5 The Review also suggested that more detailed guidance be developed:

- on the format, timing, and readability of notices and policies,[441] and
- to provide standardised templates and layouts for privacy policies and collection notices, and standardised terminology and icons, to enhance consumers' ability to understand them.[442]

5.4.6 The Privacy Act Review recommended the introduction of an additional requirement for an APP entity to 'take reasonable steps to satisfy itself that … information was originally collected from the individual in accordance with APP 3', where that information was not collected directly from the individual. It also recommended the development of OAIC guidelines that provide examples of reasonable steps that could be taken in this regard.[443] The Review explained that this proposal responded

[436] Privacy Act Review Report 2022 29.
[437] Ibid 30. The Privacy Act Review recommended exceptions for commercially sensitive material: see ibid 30 and ch 18.
[438] Privacy Act Review Report 2022 Proposal 10.1.
[439] Ibid Proposal 16.3 and 151.
[440] Ibid Proposals 10.2, 18.7 and 23.5.
[441] Ibid Proposal 16.3 and 151.
[442] Ibid Proposal 10.3.
[443] Privacy Act Review Report 2022 Proposal 13.4.

to concerns raised by the OAIC about entities collecting personal information from other entities, where it was 'reasonably apparent' that the original collection was unlawful, such as through a data breach.[444]

5.4.7 The Commonwealth Government agreed in-principle with each of these proposals.[445]

Collection of sensitive information (including health information)

5.4.8 The Privacy Act Review proposed the introduction of a legislative provision permitting 'broad consent' for research purposes, which would be available for all research to which the research exceptions in the Act apply, and 'would be given for "research areas" where it is not practicable to fully identify the purposes of collection, use or disclosure of personal or sensitive information at the point when consent is being obtained'.[446] This was in response to submissions arguing that the existing research exceptions only apply to health and medical research, which appeared to contribute to an under-utilisation of the exceptions for legitimate purposes.

5.4.9 The Review noted that submitters had also argued for the simplification of the research consent exceptions in the Privacy Act, on the basis that the different rules applying to agencies and organisations were confusing and constituted a hindrance to the effective conduct of research.[447] The Review proposed that further consultation be undertaken on the development of a single research exception, and a single set of guidelines, that apply to all APP entities.[448]

5.4.10 The Review also recommended further consultation on 'broadening the scope of research permitted without consent'[449] and, significantly for the present project, that further work could be conducted on the 'scope and harmonisation of research exceptions' across Australian jurisdictions.[450]

5.4.11 The Government agreed with each of these proposals.[451]

Collection of unsolicited information

5.4.12 The Privacy Act Review did not recommend any changes to the Privacy Act's approach to unsolicited information.

Use and disclosure of personal information (including sensitive information)

5.4.13 The Review proposed the introduction of an additional accountability requirement on APP entities to promote appropriate privacy risk management; namely, that they must 'determine and record' the purposes for which personal information will be collected, used, and disclosed at or before the time of collection.[452] In relation to use or disclosure for secondary purposes, the Review proposed that APP

[444] Privacy Act Review Report 2022 130.
[445] Government Response 10, 14, 16–18.
[446] Privacy Act Review Report 2022 Proposal 14.1.
[447] Ibid 138.
[448] Ibid Proposal 14.3 and 138–139.
[449] Ibid Proposals 14.2, 14.3.
[450] Ibid 138.
[451] Government Response 17.
[452] Privacy Act Review Report 2022 Proposal 15.1 and 143.

entities be required to record the secondary purpose at or before the time of undertaking the secondary use or disclosure.[453]

5.4.14 The Review explained that this could have multiple benefits, including supporting entities' demonstration of their compliance with the Privacy Act, and assessment of whether collection, use, or disclosure is 'fair and reasonable in the circumstances', and supporting their ability to respond to individual rights requests and complaints (which are discussed further below).[454] The Government agreed in-principle with this proposal.[455]

5.4.15 The Review proposed that the Privacy Act be amended to add a definition of 'disclosure', largely in response to concerns about cross-border flows of information.[456] That proposal is discussed at paragraph [5.4.20] below.

Cross-border disclosure

5.4.16 The Privacy Act Review discussed the exception to the requirement for an APP entity to take 'reasonable steps' to ensure compliance with the APPs, if it reasonably believes:

- the cross-border recipient of the information is subject to protections under a law or binding scheme which is substantially similar to the APPs; and
- there are mechanisms an individual can access to take action to enforce the protections (see [5.3.29] above).[457]

5.4.17 Submissions to the Review had expressed concern about the burden this placed on APP entities to assess whether overseas regimes met this requirement. Consequently, the Review proposed the introduction of a 'mechanism to prescribe countries and certification schemes as providing substantially similar protections to the APPs', which was supported by a large number of submitters to the review.[458] The Government agreed with this proposal.[459]

5.4.18 The Review further suggested that standard contractual clauses be made available to APP entities to assist with their Privacy Act compliance when transferring personal information to overseas entities in places that are not prescribed by the abovementioned mechanism.[460] The Government agreed in-principle with this proposal.[461]

5.4.19 The Review recommended strengthening the consent exception to the 'reasonable steps' requirement, if an APP entity has informed an individual that the requirement will not apply if they consent to overseas disclosure of their personal information. It proposed that entities be required to 'consider the risks of an overseas disclosure and to inform individuals that privacy protections may not apply to their information if they consent to the disclosure'.[462] This proposal was made in response to concerns raised by some stakeholders that the consent exception placed too much burden on individuals

[453] Privacy Act Review Report 2022 Proposal 15.1 and 143.
[454] Ibid.
[455] Government Response 10.
[456] Privacy Act Review Report 2022 Proposal 23.6.
[457] Privacy Act Review Report 2022 237.
[458] Ibid Proposal 23.2 and 238.
[459] Government Response 16.
[460] Privacy Act Review Report 2022 Proposal 23.3 and 239.
[461] Government Response 16.
[462] Privacy Act Review Report 2022 Proposal 23.4 and 239–240.

to consider privacy risks relating to overseas disclosure.[463] The Government agreed in-principle with this proposal, but stated that consideration should be given to whether a proposed fair and reasonable test (discussed at [5.4.24] below) 'may achieve this aim while providing entities with sufficient flexibility'.[464]

5.4.20 The Review also proposed that a definition of 'disclosure', based on the definition in existing OAIC guidance, be added to the Privacy Act.[465] As explained in the Final Report:

> OAIC guidance distinguishes between the concept of 'use' encompassing information handling and management activities occurring within an entity's effective control, and 'disclosure' which occurs when an entity makes information accessible or visible to others outside the entity and releases the subsequent handling of the personal information from its effective control.[466]

5.4.21 The Review stated that many submitters supported the proposal to introduce a definition of disclosure on the basis that this would help APP entities to determine the application of APP 8 in relation to overseas transfers, as well as clarifying that APP 8 does not apply to entities that provide personal information to secure cloud service providers that are located overseas.[467] The Government agreed in-principle with this proposal.[468]

5.4.22 The Review also proposed that existing APP 8 protections should be extended to de-identified information by requiring APP entities to take reasonable steps to ensure overseas recipients of de-identified information do not breach the APPs in relation to the information, 'including ensuring that the receiving entity does not reidentify the information or further disclose the information in such a way as to undermine the effectiveness of de-identification'.[469] The Government noted this proposal and undertook to 'consider further' how the objective of protecting de-identified information from unauthorised re-identification could be achieved.[470]

Additional proposals relating to collection, use or disclosure

5.4.23 The Privacy Act Review also considered matters that affect all the stages of personal information handling discussed in this Part: collection, use, and disclosure. It proposed the introduction of three overarching changes to the obligations on APP entities:

- a prohibition on collection, use, and disclosure, unless it is 'fair and reasonable in the circumstances';
- the strengthening of consent requirements in relation to specified types of collection, use, and disclosure; and

[463] Privacy Act Review Report 2022 Proposal 23.4 and 239–240.
[464] Government Response 16.
[465] Privacy Act Review Report 2022 Proposal 23.6.
[466] Privacy Act Review Report 2022 243 and citing OAIC, *APP Guidelines* [B.67], [B.71].
[467] Ibid. The Review also proposed that further consideration be given to whether online publications of personal information should be excluded from the APP 8 cross-border disclosure requirements were it is in the public interest: Proposal 23.6.
[468] Government Response 15.
[469] Privacy Act Review Report 2022 Proposal 4.6(b).
[470] Government Response 5.

- the introduction of an individual 'right to object' to the collection, use, or disclosure of personal information; that is, 'a right to challenge whether an APP entity's handling of information complies with the Act'.[471]

Fair and reasonable test

5.4.24 The Review recommended amendments to the Privacy Act extend the existing requirement that collection of personal information be by 'fair means' in APP 3 (discussed in [5.3.4] above) to also apply to the use and disclosure of information. The Review recommended that this take the form of a limitation on collection, use, and disclosure of personal information to situations where it is 'fair and reasonable in the circumstances'.[472] This was 'generally supported by submitters' on the basis that it would ensure information handling was not harmful and was aligned with individuals' reasonable expectations.[473] The Privacy Act Review noted that most submitters considered that growing digital privacy risks would not be adequately addressed through enhanced disclosure and consent requirements (which require individuals to read potentially large volumes of information and assess current and future risks) and required the imposition of minimum standards governing information handling.[474]

5.4.25 The Review further recommended that the Privacy Act be amended to include a list of considerations that may be taken into account in determining whether a collection, use, or disclosure is fair and reasonable in the circumstances. These include:

- 'whether an individual would reasonably expect the personal information to be collected, used or disclosed';
- 'the kind, sensitivity and amount of personal information being collected, used or disclosed';
- 'whether the collection, use or disclosure is reasonably necessary for the functions and activities of the organisation or is reasonably necessary or directly related for the functions and activities of the agency';
- 'the risk of unjustified adverse impact or harm';
- 'whether the impact of privacy is proportionate to the benefit';
- 'if the personal information relates to a child, whether the collection, use or disclosure of the personal information is in the best interests of the child'—on the basis that this would provide greater privacy protections for children and would allow for better balancing of children's rights to safety and privacy with rights relating to information, expression and education; and
- the objects of the Privacy Act.[475]

5.4.26 The Review proposed that the fair and reasonable requirement should apply regardless of whether consent had been obtained.[476] However, it proposed that the requirement should not apply to certain the exceptions relating to the collection of sensitive information or the use and disclosure of personal information, such as collection, use, or disclosure required or authorised by law or a

[471] Privacy Act Review Report 2022 166.
[472] Ibid Proposal 12.1. This amendment would necessitate the removal of the reference to 'fair means' of collection in APP 3: Proposal 12.3.
[473] Ibid 3.
[474] Ibid 111–112.
[475] Privacy Act Review Report 2022 Proposals 12.2 and 16.4, and 120, 152.
[476] Ibid Proposal 12.3.

court/tribunal order, relating to enforcement activities, or relating to permitted health purposes, among others.[477] The Government agreed in-principle with each of these proposals.[478]

Consent to collection, use, or disclosure

5.4.27 The Privacy Act Review also considered whether there should be changes to the way consent to information-handling is defined, and the circumstances in which it should be obtained, in the Privacy Act. This included consideration of the existing requirement for individuals to consent to the collection of sensitive information (unless an exception applies), to consent to APP entities' use or disclosure of personal information for a secondary purpose, or to consent to overseas disclosure of personal information.[479]

5.4.28 The Review rejected the recommendation in the ACCC's DPI Report that consent should be required for all collection, use, and disclosure of personal information, unless the information is 'necessary for performance of a contract to which the consumer is a party … is required under law, or is otherwise necessary for an overriding public interest reason'.[480] The Review stated that there was 'broad agreement' among submitters that consent 'is most effective when used in a narrow range of situations where individuals most need to exert control over their personal information'.[481]

5.4.29 Consequently, the Review proposed more modest changes to 'improve the quality of consent obtained from individuals'. These were largely in response to concerns about online privacy—such as the use of 'choice architecture', 'dark patterns', or vague or complex wording to influence or confuse users in a manner that detracts from effective consent.[482]

5.4.30 The Review proposed that the Privacy Act definition of consent be amended to specify that consent 'must be voluntary, informed, current, specific, and unambiguous'.[483] The Government agreed in-principle with this proposal.

5.4.31 In response to concerns raised about children's consent under the Act (discussed further at [5.4.36] below), the Review further proposed that the Act also be amended to clarify that an individual's consent will only be valid if the person has capacity' that is, 'if it is reasonable to expect that an individual to whom the organisation's activities are directed would understand the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting'.[484]

5.4.32 The Review claimed that this would also benefit individuals experiencing vulnerability by ensuring that any such vulnerability is identified and, where appropriate, to allow for the provision of supported or substituted decision-making for people deemed unable to give valid consent on their own.[485]

5.4.33 The Review noted that it had received submissions seeking further clarity on the appropriate role of guardians and other third parties in consent and other processes prescribed under the Privacy

[477] APP 3.4, 6.2(b)-(e). Privacy Act Review Report 2022 Proposal 12.3 and 121.
[478] Government Response 8, 13.
[479] Privacy Act Review Report 2022 102.
[480] ACCC, *DPI Report* Recommendation 16(c), 464; Privacy Act Review Report 2022 102.
[481] Privacy Act Review Report 2022 102 and citing numerous submissions to its Issues Paper.
[482] Privacy Act Review Report 2022.
[483] Ibid 11.1 and 104.
[484] Ibid Proposal 16.2 and 163–164.
[485] Ibid 162.

Act, including in relation to complex situations where the third party may be contributing to the person's vulnerability, such as domestic and family violence situations.[486] It further noted recent changes in 'understanding how to promote the rights of people with disabilities and reduced decision-making capacity', which involve maximising the recognition of all people's right to be recognised and to act as legal persons, and to access support they may need to do this. The Review proposed that the OAIC update its guidance on capacity and consent to reflect current thinking on supported decision-making.[487] The Government agreed with this proposal.[488]

5.4.34 The Review also proposed that the Privacy Act be amended to expressly recognise that all individuals can withdraw consent (and that this should be as easy as it was to give consent), with the proviso that withdrawal does not affect the lawfulness of how the information was handled prior to the withdrawal.[489] The Government agreed in-principle with this proposal.[490]

5.4.35 In relation to online services, the Review further proposed (and the Government agreed in-principle)[491] that:

- OAIC guidance be developed on how online services should design consent requests (on the basis that these could improve consumers' decision-making and understanding of how data is handled);[492] and
- 'APP entities that provide online services should be required to ensure that any privacy settings are clear and easily accessible for service users'.[493]

Consent of children

5.4.36 The Privacy Act Review considered several issues relating to children's privacy and sought responses to proposals for the introduction of child-specific privacy protections in the Privacy Act, largely in response to concerns about online privacy risks.[494] The Review reported that submitters had acknowledged the increasingly 'online' nature of children's lives and the benefits to children of online services and platforms, including enabling them to exercise rights to access information, freedom of expression, and freedom of association.[495] Submitters to the Review also expressed concerns that these interactions enable entities to collect large amounts of data and build profiles on children that can be used to target them (including when they are most vulnerable) and can be shared or sold.[496]

[486] Privacy Act Review Report 2022 162.
[487] Ibid Proposal 17.2 and 164.
[488] Government Response 14. Note that Part 9 of this Report discusses other contexts relating to safety in which information sharing has been identified as important.
[489] Privacy Act Review Report 2022 Proposal 11.3 and 106–107.
[490] Government Response 17.
[491] Ibid 8, 17.
[492] Privacy Act Review Report 2022 Proposal 11.2 and 106.
[493] Ibid Proposal 11.4 and 109. The Review proposed that '[o]nline privacy settings should reflect the privacy by default framework in the Act', which the OAIC described as an approach 'that requires entities to ensure that, by default, personal information is handled with the highest privacy protections': OAIC, *Privacy Act Review: Issues Paper Submission* (11 December 2020) [7.14] <https://www.oaic.gov.au/__data/assets/pdf_file/0018/1773/privacy-act-review-issues-paper-submission.pdf> and citing European Commission, *What Does Data Protection 'By Design' and 'By Default' Mean?* (Web Page, 2023) <https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-does-data-protection-design-and-default-mean_en>.
[494] Privacy Act Review Report 2022 146.
[495] Ibid.
[496] Privacy Act Review Report 2022 146.

5.4.37 The Review recommended that the Privacy Act define 'a child' as 'an individual who has not yet reached 18 years of age',[497] and expressed the view that existing OAIC guidance on assessing capacity and obtaining consent in relation to children's personal information is appropriate.[498] That guidance instructs APP entities to assess children's capacity on a case-by-case basis and, if that is not practical, to assume children over the age of 15 have capacity, unless something suggests otherwise.[499]

5.4.38 As noted at [5.4.31] above, the Review proposed that the Act be amended to clarify that consent will only be valid if it is given by an individual with capacity. The Review recommended that exceptions to this requirement be codified 'for circumstances where parent or guardian involvement could be harmful to the child or otherwise contrary to their interests (including, but not limited to confidential healthcare advice, domestic violence, mental health, drug and alcohol, homelessness or other child support and community services)'.[500]

5.4.39 To address broader children's privacy issues relating to online services, the Review proposed the development of a Children's Online Privacy Code, in consultation with children, parents, experts, advocates, and industry. This could be based on the UK's Age Appropriate Design Code and would 'address how the best interests of child users should be supported in the design of an online service', including matters such as whether there should be specific requirements for assessing capacity, whether certain information handling should be limited, and how privacy information (such as collection notices and privacy policies) should be designed to improve accessibility.[501]

Right to object

5.4.40 The Privacy Act Review recommended the creation of a right to object to the collection, use, or disclosure of personal information. This is related to, but distinct from, the proposed right to withdraw consent discussed above in section [5.4.34].

5.4.41 The right proposed in the Privacy Act Review was modelled on the corresponding right in the GDPR. Under Article 21 of the GDPR, individuals have a right to object to the processing of their personal information. This right applies alongside fairness and reasonableness requirements in circumstances where there is no requirement for an individual to consent to the collection and use of their information. The GDPR right creates an absolute right to challenge the processing of personal data for direct marketing purposes, and a more qualified 'right to question or challenge' that obliges a regulated entity handling data for its legitimate interests or a public task to either demonstrate a compelling reason to continue processing or to cease doing so.[502]

5.4.42 The Review's proposed right to object for the Privacy Act would similarly create a right for individuals to challenge an APP entity's handling of personal information in terms of the requirements of the Privacy Act. As the Review explained in its Final Report:

---

[497] Privacy Act Review Report 2022 Proposal 16.2.
[498] The Review considered, and sought submissions on, several options for a more appropriate consent mechanism for the handling of children's information, including the ACCC's recommendation in the DPI Report that all handling of personal information of children under 16 should only be permitted with the consent of a guardian or a narrower requirement for a guardian's consent to handling a child's information where consent is currently required in the Privacy Act: ACCC, *DPI Report* 468, drawing on art 8 of the GDPR and also the United States' *Children's Online Privacy Protection Act 1998*: 15 USC §§ 6501–6506 (1998); Privacy Act Review Report 2022 147.
[499] Ibid Proposal 16.2.
[500] Ibid Proposal 16.2 and 149.
[501] Ibid Proposal 16.5.
[502] Privacy Act Review Report 2022 172.

> It would require an APP entity to review its information-handling in light of the objection and provide a response to the objection. For example, an individual could challenge an entity that a particular collection is not reasonably necessary and/or not fair and reasonable.[503]

5.4.43 Successful outcomes of objections might include an APP entity minimising collection, collecting different information, or modifying its use and disclosure practices in relation to certain information. Alternatively, an APP entity's response to an objection may equip the individual with useful information for deciding whether to deal with the entity or to pursue redress in relation to other rights (which are discussed in Part 6 of this Report).[504]

5.4.44 The Review recommended that several general exemptions should be available in relation to this and other proposed individual rights, including exemptions in the public interest, exemptions where required or authorised by law and legal relationships, and exemptions there is an abuse of process. These are discussed in [6.4.20]–[6.4.25] of this Report.

5.5 Consultation

5.5.1 The TLRI Issues Paper posed two questions relating to the regulation of collection, use, and disclosure of personal information in the PIPPs:

> Are there any other amendments to the PIPPs that you think should be made?[505]
>
> Should any of the other potential reforms be introduced, including:
>
> > fairness and reasonableness requirements;
> >
> > …
> >
> > strengthened notice and consent requirements?[506]

Collection of personal information

5.5.2 Meg Webb MLC submitted that the PIPPs should be amended to be consistent with the APPs in requiring 'that notice of the circumstances of the data collection must be provided prior [to] collection, as well as disclosure [of] who else may have access to that data once collected' on the basis that these elements are key to gaining informed consent.[507]

5.5.3 Ms Webb also recommended the introduction of a requirement for collecting authorities to 'indicate the duration that it is intended for that personal information to remain stored, accessible and used'. This recommendation was made on the basis that there would be times where personal information will only be used or pertinent for a defined period, and that it would facilitate erasure, and notice of erasure to affected people (see also the discussion of the right to erasure at [6.3]–[6.6] of this Report). Ms Webb gave the example of the Check-In Tas app used for contact tracing during the early years of the COVID-19 pandemic, which specified that data would only be kept for 28 days.

---

[503] Privacy Act Review Report 2022 172.
[504] Ibid.
[505] Issues Paper Part 2, Question 2.8.
[506] Ibid Part 2, Question 2.9(a) and (e).
[507] Submission 8 (Meg Webb MLC).

Collection, use, and disclosure of personal information

5.5.4 Professor Margaret Otlowski, Emeritus Distinguished Professor Dianne Nicol, and Dr Lisa Eckstein of the Centre for Law and Genetics expressed support for the Privacy Act Review Report's proposal for the introduction of a requirement that collection, use, or disclosure of personal information must be fair and reasonable in the circumstances, and recommended a similar reform be made to the PIPA.[508]

5.5.5 Meg Webb MLC expressed strong support for the amendment of the PIPA to align with the APPs in requiring collection of personal information to be both lawful and fair.[509] Ms Webb acknowledged that the flexibility the PIPA provides in relation to health information, including options to disclose health information on behalf of individuals who are unable to provide or communicate consent, may be appropriate on the basis of practicality, provided they are supported by appropriate oversight and reporting mechanisms.[510] The latter are discussed further in Part 5 of this Final Report.

5.5.6 Richard Griggs observed that the PIPPs permit the collection and/or use and disclosure of personal information (generally or for a secondary purpose) where it is, for instance, 'by lawful means', 'authorised or required by law' or 'required or permitted by law'.[511] Mr Griggs argued that these 'can operate as an exemption mechanism', meaning they can be used 'by government to add to its own functions or activities and change and expand what they are authorised to do with the personal information'. Mr Griggs cited the Tasmanian Government's use of this mechanism, via the creation of regulation, to permit the Tasmanian Government to share Tasmanian drivers licence photographs with the Commonwealth Government for the proposed National Driver Licence Facial Recognition Solution ('NDLFRS') (described above at [4.9]). Mr Griggs recommended that the 'authorised or required by law' exception be amended to clarify that it only applies to law passed by State Parliament.[512]

5.5.7 Dr Joel Scanlan noted that the creation of a right to object, and greater transparency, were positive developments in the GDPR.[513]

Consent to collection, use, or disclosure

5.5.8 The Centre for Law and Genetics team expressed concern about the Privacy Act Review's proposal to define 'consent' to mean 'voluntary, informed, current, specific and unambiguous' consent, on the basis that this may 'impede ethically acceptable research'.[514] The Centre expressed a preference for consent options to be based on individual choice, while also being 'structured so as to facilitate various forms of consent', noting the 'broad consent' approach now used in genomic research.

5.5.9 Youth Law Australia ('YLA') raised the issue of consent given by children. It submitted that it is not always appropriate for consent relating to a child's information to be obtained through their parent or guardian (and may in some circumstances not be safe or protective or may be contrary to the child's best interests).

5.5.10 YLA argued against the imposition of such consent requirements, or of a high age for capacity to consent (such as 16 years of age), on the basis that this 'reflects an assumption that children lack the

[508] Submission 17 (Centre for Law and Genetics).
[509] Submission 8 (Meg Webb MLC).
[510] Ibid.
[511] See, eg, PIPP 1(f), 7(4)(a); PIPP 9(e); PIPP 10(1)(b).
[512] Submission 10 (Richard Griggs).
[513] Submission 20 (Dr Joel Scanlan).
[514] Submission 17 (Centre for Law and Genetics).

capacity to protect their own interests and are dependent on adults to make decisions in their own interests', and that it reinforces existing difficulties for children and young people seeking to enforce their privacy rights.[515] YLA instead proposed an approach based on 'scaffolding' and context, and submitted that best practice requires an approach that maximises children and young people's participation in decisions, even where they may not have capacity to consent to collection, use, and disclosure of their personal information.[516]

5.5.11 The Commissioner for Children and Young People observed that children's use of online services and platforms presents both opportunities and risks. The Commissioner noted that adults play a role in helping uphold the rights of children and young people, including their right to privacy, which makes questions about children's privacy more complex. The Commissioner further argued that children must be involved in the development of any new or revised privacy protections affecting them, to ensure that any changes are informed by a proper understanding of the implications of privacy on their lives.[517]

5.6 The TLRI's view

5.6.1 The TLRI's view is that the Tasmanian privacy principles concerning the collection, use, and disclosure of personal information (PIPPs 1, 2 and 9) do, in the main, provide adequate privacy protection. However, in light of submissions received in response to the Issues Paper and developments in other jurisdictions—especially the recent Commonwealth Privacy Act Review—the TLRI recommends a number of changes to the PIPPs and other provisions of the PIPA to enhance consistency and clarity for both individuals and personal information custodians and to respond more comprehensively to privacy risks associated with the increasing proliferation and sophistication of digital technology.

Collection of personal information

5.6.2 The TLRI considers there may be a benefit to defining the term 'collects' in the PIPA and aligning it with the Privacy Act Review's proposed amendment to the Privacy Act definition. This would clarify that the protections relating to collection of personal information apply to inferred and generated information (see [5.4.1] and following). While no submissions to the TLRI Issues Paper raised this matter, such a change would arguably be consistent with more general calls from several submitters to ensure that the PIPA is equipped to deal with contemporary and emerging privacy risks associated with technological advances.[518]

5.6.3 The TLRI considers that it would enhance transparency for individuals if PIPP 1(3) were amended to align more closely with APP 5 by requiring personal information custodians to disclose who else may have access to personal information, including cross-border recipients.[519]

5.6.4 The TLRI observes that the wording of PIPP 1 in relation to the timing of reasonable steps to give notice of collection—'either before collection, during collection or as soon as practicable after collection'—is potentially weaker than the equivalent requirement in the Privacy Act, which requires

[515] Submission 12 (Youth Law Australia) 3.
[516] Ibid.
[517] Submission 21 (Commissioner for Children and Young People).
[518] See, eg, Submission 8 (Meg Webb MLC); Submission 5 (Tasmania Legal Aid); Submission 10 (Richard Griggs); Submission 11 (TasCOSS).
[519] *Privacy Act 1988* (Cth) sch 1, cl 5.2.

reasonable steps to give notice '[a]t or before the time of collection or, if that is not practicable, as soon as is practicable after collection'.[520] The TLRI recommends that the wording in the Privacy Act be adopted for the PIPA, on the basis that this would encourage custodians to prioritise notice before or during collection, and only resort to notice after collection where earlier notice is impracticable.

5.6.5 The TLRI considers that the proposed amendments to strengthen collection notice requirements in the Privacy Act Review's Final Report may also be appropriate for the PIPA. This is because they could support personal information custodians' decision-making and compliance, as well as enhance transparency for individuals and equip them to better assert their privacy rights. The TLRI recommends these matters be given further consideration in light of the Commonwealth review:

- whether the PIPA should specify that collection notices should be clear and understandable (including where addressed to a child), and accessible;[521] and
- whether collection notices should contain additional details, such as details of the circumstances of handling where a high-risk activity is involved, information about the privacy policy and what it contains, and types of information that may be disclosed to cross-border recipients.[522]

5.6.6 The TLRI notes Meg Webb MLC's suggestion that 'collecting authorities' should also indicate the intended duration of storage, accessibility, and usage of personal information. The TLRI observes that such a requirement does not apply in other Australian jurisdictions. The Commonwealth Privacy Act Review did make related proposals that APP entities should be required to establish retention periods for personal information and state them in their privacy policies; these recommendations and their significance for the PIPA are addressed in Parts 6 and 7 below.

5.6.7 The TLRI observes that PIPP 1 and APP 3 are phrased differently in terms of the circumstances in which personal information custodians or APP entities can collect information about an individual from someone other than the individual. Specifically, PIPP 1 states that personal information custodians must collect information from the individual, if it is reasonable and practicable to do so. APP 3 similarly holds that agencies must collect personal information from the individual, unless it is unreasonable or impracticable to do so, but also specifically permits collection from someone else where the individual consents or where the agency is required or authorised to do so.

5.6.8 The TLRI notes that legislation in other jurisdictions takes varying approaches; for example, the Victorian legislation expresses a principle nearly identical to PIPP 1,[523] while the NSW legislation, like the Privacy Act, permits collection from another party, where this was authorised by the individual.[524]

5.6.9 The TLRI's view is that there may be value in aligning PIPP 1 with APP 3 by enabling custodians to collect personal information from another person, where the individual concerned has consented or where the custodian is required by law to collect the information.[525]

5.6.10 If such an amendment is made, there is a need to consider the scope of protections, such as the proposal in the Privacy Act Review Final Report that APP entities should be required to take

[520] *Privacy Act 1988* (Cth) sch 1, cl. 5.1.
[521] Privacy Act Review Report 2022 Proposals 10.1 and 16.3.
[522] Ibid Proposal 10.2.
[523] *Privacy and Data Protection Act 2014* (Vic) sch 1, cl 1.4.
[524] *Privacy and Personal Information Protection Act* 2009 (NSW) s 9. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[525] *Privacy Act 1988* (Cth) sch 1, cl 3.6.

reasonable steps to satisfy themselves that information collected from someone other than the individual was originally collected from the individual in accordance with the relevant APP.

5.6.11 Individuals' consent to collection from third parties, and to other information handling that requires consent under the PIPPs,[526] must be valid. The TLRI considers it would be appropriate to amend the PIPA to define consent, using the definition of valid consent currently set out in the OAIC Guidelines on the Australian Privacy Principles. This corresponds with the Privacy Act Review's proposal for amending the definition of consent in the Privacy Act.

5.6.12 In light of the growing use of online consent processes by public and private entities, the TLRI also considers that the development of guidance on the design of consent requests for online services, recommended by the Privacy Act Review for entities bound by the Commonwealth legislation, could also be beneficial for Tasmanian personal information custodians.[527]

Collection of sensitive information (including health information)

5.6.13 The TLRI observes that PIPP 10, unlike APP 3, does not permit the collection of sensitive information for the purpose of a confidential alternative dispute resolution process. The TLRI has not received information or submissions about the significance, if any, of this difference in practice and, accordingly, makes no recommendations.

5.6.14 The TLRI also observes that there are some minor differences between the PIPA and the Privacy Act in the exceptions to the consent requirement relating to the provision of health services. For example, the Privacy Act (but not the PIPA) permits collection from a third party where the information is about family, social *or medical* history, whereas the PIPA only applies to family and social history.[528] The TLRI did not receive any submissions on this point and also makes no recommendations.

Collection of unsolicited information

5.6.15 The TLRI observes that the explicit exclusion of unsolicited information from the PIPP 1 collection requirements[529] means that personal information custodians are not obliged to inform an individual that the custodian holds their unsolicited personal information. The practical effect of this appears to be that a personal information custodian can use unsolicited information, even in circumstances where it could not have collected the information directly, and where the individual does not know the custodian has the information. Further, the PIPPs do not create a clear obligation for custodians to destroy or de-identify unsolicited information.[530]

5.6.16 The TLRI observes that PIPPS 2–10 (discussed in this Part) apply by default to unsolicited personal information. However, three of these—PIPP 2 (on use and disclosure), PIPP 3 (on data quality), and PIPP 10 (on sensitive information)—assess the permissibility of handling by reference to

[526] As set out at varying points in this Part, various PIPPs allow the handling of an individual's personal information based on the provision of consent by the individual. Consent can be the basis for using personal information for a secondary purpose in PIPP 2, using unique identifiers in PIPP 7, disclosing information outside of Tasmania in PIPP 9, and collecting sensitive information under PIPP 10. The PIPA does not define what amounts to 'consent'.
[527] Privacy Act Review Report 2022 Proposal 11.2 and 106.
[528] *Privacy Act 1988* (Cth) s 16B(1A); cf PIPA sch 1, PIPP 10(6).
[529] PIPA s 11.
[530] PIPP 4 provides for destruction or de-identification only where the information is no longer needed for any purpose: PIPA sch 1.

the purpose of collection. It is unclear how these PIPPs would apply to unsolicited information, given that no objective purpose of collection exists in such circumstances.

5.6.17 The TLRI notes that the NSW legislation is similar to the PIPA in stating that personal information is not 'collected' if it is received unsolicited.[531] Legislation in other jurisdictions, such as Victoria and Queensland, does not mention unsolicited information at all.[532] In contrast, the Privacy Act's APP 4 establishes an approach that provides the same level of protection to unsolicited information as is afforded to other forms of personal information. The Privacy Act Review did not propose any changes to this provision.

5.6.18 The TLRI did not receive any submissions on this issue. Nevertheless, in light of the apparent gap in privacy protections relating to unsolicited information, the TLRI recommends that PIPP 1 should be amended to specify how personal information custodians should respond to receiving unsolicited information in a manner similar to APP 4.

Use and disclosure of personal information (including sensitive information)

5.6.19 The TLRI observes that there are some minor differences between the PIPPs and the APPs in terms of the secondary purposes for which disclosure of personal information is permitted. Most notably, unlike the APPs, the PIPPs do not permit disclosure of personal information where it is reasonably necessary for a confidential alternative dispute resolution process. This was mentioned in the Issues Paper for this project, but no consultation questions were posed, or submissions received, on it. Accordingly, the TLRI makes no recommendation.

5.6.20 The TLRI observes that the PIPA is broader than the Privacy Act in the scope of the exception to the prohibition on secondary use or disclosure, with the PIPA permitting such practices for research in the public interest, rather than only for research relevant to public health or safety. The TLRI notes that the Privacy Act Review Report proposed (and the Government agreed) that further consideration be given to broadening the research exceptions in the Privacy Act (discussed above at [5.4.8] and following), indicating that the Privacy Act may in the future be amended to align more closely with the PIPA.

5.6.21 The TLRI also notes that the Privacy Act presently provides stronger privacy protection for employee information held by public agencies than does the PIPA, the latter of which creates an exception to the consent requirement for use and disclosure of employee information for employment purposes. The Privacy Act exception is presently only available for non-public sector organisations, but the Privacy Act Review recommended that privacy protections be extended to these organisations. This is discussed, and recommendations are made, in [3.4] of this Report.

Cross-border disclosure

5.6.22 The TLRI considers that the PIPA should be amended to align more closely with existing Privacy Act protections relating to cross-border disclosure. Such reforms would ensure consistency, and promote greater privacy protections, relating to:

[531] *Privacy and Personal Information Protection Act 1998* (NSW) s 4(5).
[532] However, it is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) will include a QPP that deals with unsolicited personal information, (QPP 4) (yet to be commenced).

- whether personal information custodians should be required to hold a reasonable belief that there are mechanisms for the individual to enforce existing privacy protections prior to cross-border disclosure;[533]
- whether personal information custodians should be required to expressly inform individuals that, if the individual consents to cross-border disclosure, the custodian will not be obliged to take reasonable steps to ensure the recipient does not breach the PIPPs[534] (and, per the Privacy Act Review's further proposal, that privacy protections may not apply to the recipient);[535] and
- whether personal information custodians retain responsibility for breaches of the PIPPs after they have taken reasonable steps to ensure the recipient deals with the information consistently with the PIPPs.[536]

5.6.23 The TLRI recommends that the PIPA be amended to include a definition of 'disclosure' based on existing OAIC guidance, in line with the Privacy Act Review's proposal for amending the Privacy Act (with which the Commonwealth Government agreed in-principle). This would clarify that PIPP 9 does not apply to entities that provide personal information to secure cloud service providers located outside Tasmania, on the basis that this constitutes 'use' rather than 'disclosure' and so is protected under other PIPPs.[537] The TLRI notes that other proposals of the Privacy Act Review—namely, that a mechanism to certify countries that provide similar protection to the Privacy Act, and standard contractual clauses that would constitute 'reasonable steps' where disclosure is to a non-certified country—could also assist Tasmanian personal information custodians to comply with the PIPA in relation to overseas disclosures (see paragraph [5.4.17] above).[538]

Collection, use, and disclosure generally

5.6.24 The TLRI observes that the PIPA currently only requires personal information custodians to collect information by lawful means. This is the same test as applies in NSW,[539] which is a lower standard than applies to the collection of personal information under the Privacy Act (which must be by 'fair means') and similar provisions in other jurisdictions, such as Queensland and Victoria.[540] It is also considerably lower than the standard of 'fair and reasonable in the circumstances' that was proposed by the Privacy Act Review as a test that should apply to collection, use, and disclosure of information under the Commonwealth legislation.

5.6.25 As discussed above at [5.4.24], the Privacy Act Review agreed with submitters that, in the context of emerging digital privacy risks, it is appropriate to place greater obligations on information handlers to consider the impacts on individuals, and individuals' expectations, in making decisions about collection, use, and disclosure. The TLRI observes that several submitters to the present project expressed concerns about the adequacy of Tasmanian privacy protections to deal with emerging digital risks.[541]

---

[533] APP 8.2(a)(ii).
[534] APP 8.2(b).
[535] Privacy Act Review Report 2022 Proposal 23.4 and 239–240.
[536] *Privacy Act 1988* (Cth) s 16C.
[537] Privacy Act Review Report 2022 Proposal 23.6.
[538] Ibid Proposal 23.2 and 238.
[539] *Privacy and Personal Information Protection Act 1998* (NSW) s 8.
[540] *Information Privacy Act 2009* (Qld) sch 3 cl 1(2); *Privacy and Data Protection Act 2014* (Vic) sch 1, cl 1.2. In Queensland, the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) will specify that collection is by lawful and fair means (yet to be commenced).
[541] For example, Submission 5 (Tasmania Legal Aid); Submission 8 (Meg Webb MLC); Submission 10 (Richard Griggs); Submission 18 (Dr Sarah Moulds).

5.6.26 In the TLRI's view, incorporating a 'fair and reasonable' standard for the collection, use, and disclosure of all forms of personal information into the PIPA, along with a set of guiding criteria for applying the standard, would enable Tasmania to better regulate the collection, use and disclosure of personal information. This would be consistent with, and in some respects exceed, the protection provided by the 'fair means' test that currently applies to collection of personal information under the Privacy Act and the Queensland and Victorian Acts. It would align with the proposed reform in the Privacy Act Review.

5.6.27 The TLRI notes the Privacy Act Review Report's proposal to require APP entities to determine and record the purposes of collection, use, and disclosure of personal information, including any secondary uses or disclosures, at or before the time of collection or of undertaking the secondary use or disclosure.[542] The TLRI recommends that a corresponding amendment to PIPP 1 should be made, on the basis that it would support personal information custodians to comply with the PIPPs, to review and report on that compliance, and to respond to complaints or concerns (discussed further in Part 6 of this Report).

Required or authorised by law

5.6.28 The TLRI's view is that there is a lack of clarity in the scope of the exception to the prohibition on secondary use or disclosure of personal information where 'it is required or authorised by or under law' (under PIPP 2), the exception to the prohibition on collection of sensitive information where it 'is required or permitted by law' (under PIPP 10), and similar exceptions found in other PIPPs.[543] Specifically, it is unclear whether the legal authorisation must be under legislation in order for an exception to apply, or whether it extends to authorisation under statutory instruments or contractual obligations created by custodians themselves. Further, the use of different but related terminology (for instance, in PIPP 2 and PIPP 10) raises questions about whether the two exceptions have a different scope.[544]

5.6.29 The TLRI observes that the Privacy Act contains similar exceptions, using similar wording (albeit confined to 'Australian law'), in several of the APPs, including APP 3 relating to collection of personal information and APP 6 relating to use and disclosure of personal information.[545] This also reflects the approach in other Australian jurisdictions.[546]

5.6.30 OAIC guidelines to the Privacy Act provide guidance on the interpretation of the Commonwealth exceptions.[547] The guidelines indicate that 'required' means an entity has no choice but to use or disclose the information, while 'authorised' means the entity is permitted, but not required, to do so. However, the guidelines clarify that an act or practice will not generally be 'authorised' where there is merely a *lack* of prohibition on use or disclosure, or where it relies 'solely on a general or incidental authority conferred by statute upon an agency to do anything necessary or convenient for, or incidental to or consequential upon, the specific functions and powers of the agency'.[548] Australian law

[542] Privacy Act Review Report 2022 Proposal 15.1 and p. 143.
[543] PIPA sch 1, PIPP 2(1)(f); PIPP 10(1)(b).
[544] PIPA sch 1, PIPP 2(1)(f).
[545] For example, APP 2.2(a), APP 3.4(a), APP 3.6(a)(ii), APP 5.2(c), APP 6.2(b), APP 8.2(c), APP 9.1(a), APP 9.2(c), APP 12.3(g).
[546] For example, *Privacy and Data Protection Act 2014* (Vic) sch 1, cl 2.1(f), 6.1(g); *Information Privacy Act 2009* (Qld) sch 3, cl 2(3)(b), 6(2), 10(1)(c), 11(1)(d); *Privacy and Personal Information Protection Act 1998* (NSW) ss 19(2)(h), 25. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[547] OAIC, *Australian Privacy Principles Guidelines* ch B.
[548] OAIC, *Australian Privacy Principles Guidelines* 27.

is defined as statutes, regulations, or other instruments made under such an Act and rules of the common law or equity.[549]

5.6.31 On this basis, the TLRI considers that the scope of existing PIPA information handling exceptions relating to requirement or authorisation under law should be clarified through, for example, the development of guidance similar to the OAIC guidance published in the relation to the Commonwealth Act.

Consent generally

5.6.32 Individuals can consent to the collection or use and disclosure of certain personal information that would otherwise be prohibited under the PIPA (see [5.2.20]). However, the TLRI echoes the views expressed in the Privacy Act Review Final Report that, while consent plays an important role in some elements of privacy protection in the PIPA, over-reliance on consent as a mechanism for protecting individuals' privacy is problematic and risks placing disproportionate responsibility on individuals.[550]

5.6.33 The TLRI's view is that the introduction of a clear definition of consent in the PIPA could help ensure that, where consent is required, it is genuine. On this basis, the TLRI recommends that the amendments to the definition and treatment of 'consent' relating to collection, use and disclosure of personal information set out in the Privacy Act Review Final Report (see [5.4.30] above) be implemented in the PIPA.

5.6.34 The TLRI observes that some submissions in response to the Issues Paper, and to the Privacy Act Review, raised concerns that more prescriptive consent requirements, including via the definition of consent recommended above, might interfere with ethical and publicly beneficial research. The TLRI considers that exceptions to standard consent requirements for research purposes are necessary and appropriate.

5.6.35 The TLRI recommends that further consideration be given to the introduction in Tasmania of the 'broad consent' option proposed by the Privacy Act Review,[551] and that the Tasmanian Government participate in any future work on the 'scope and harmonisation of research exceptions' across Australian jurisdictions[552] proposed by the Privacy Act Review.

Consent of children

5.6.36 As noted above, the Privacy Act Review emphasised that relying on consent to validate information handling practices runs the risk of placing responsibility on individuals rather than requiring information handlers to modify their practices.[553] This has particular significance in relation to consent of children and young people to handling of their personal information.

5.6.37 The TLRI also observes that the PIPA does not contain child-specific privacy protections. It only contemplates consent for handling of children's or young people's personal information to a limited extent; namely, in the provisions relating to consent and disclosure of personal information about an individual who lacks capacity (discussed at [5.2.21] above). This is similar to the Privacy Act provisions but stands in contrast to the privacy principles in NSW, which explicitly permit the collection

[549] Ibid [B.136].
[550] Privacy Act Review Report 2022 3.
[551] Ibid Proposal 14.1.
[552] Privacy Act Review Report 2022 138.
[553] Ibid 147.

of information from a person's parent or guardian where the individual concerned is under the age of 16.[554]

5.6.38 The TLRI agrees with several submitters in response to the Issues Paper that privacy regulation in Tasmania does not give adequate consideration to contemporary privacy risks affecting children, to the need to balance children's rights to privacy and safety with their other rights (such as their rights to information, communication and free expression),or to the evolving capacities of children and young people.

5.6.39 The TLRI observes that changes similar to the proposals of the Privacy Act Review could address some of these issues with the PIPA in Tasmania. These include:

- codification of the proviso that consent to information handling will only be valid where the individual has capacity to consent;
- exceptions to consent requirements, where seeking consent from a parent or guardian would be inappropriate or harmful for the child or young person; and
- publication of guidance for custodians to assess the capacity of children and young people on a case-by-case basis and to assume capacity for people aged 15 years and over.

5.6.40 The TLRI considers that further consultation with stakeholders, including children and young people themselves, is necessary to ensure that such amendments would be appropriate to the Tasmanian position and are consistent with contemporary understandings of children's decision-making capacity.

5.6.41 The TLRI shares the view of the Privacy Act Review that a Children's Online Privacy Code, developed through consultation with children and young people, parents and guardians, and all other relevant stakeholders, could also enhance privacy protections for children and young people around Australia.[555]

5.6.42 The TLRI also shares the view of the Privacy Act Review that guidance could assist regulated entities to ensure that they are aware of contemporary understandings of consumer vulnerability, consent, capacity, and supported decision-making to ensure that adults who might otherwise be deemed to lack capacity (such as some adults with cognitive disability) are supported to maximise their involvement in privacy-related decisions.[556]

Right to object

5.6.43 In the TLRI's view, a general right to object under the PIPA could usefully apply to a range of situations, including any use of personal information for direct marketing by non-government bodies, which is currently not addressed in the PIPPs.

5.6.44 The right to object would also allow individuals to object where government entities have collected information from a source other than the individual concerned, without the individual's consent; for example, where the government is using profiles of individuals based on information about their previous choices or browsing habits. If an objection is raised, the entity would then need to identify a compelling legitimate reason before it could continue using the information.

[554] *Privacy and Personal Information Protection Act 1988* (NSW) s 9(b).
[555] Privacy Act Review Report 2022 Proposal 16.5.
[556] Ibid Proposal 17.2 and 164.

5.7 Recommendations

Recommendation 16: The term 'collects' should be defined in the PIPA, and the definition should include inferred and generated information.

Recommendation 17: PIPP 1(3) should be amended to require personal information custodians to disclose who else may have access to the information once collected.

Recommendation 18: PIPP 1 should be amended to require personal information custodians to take reasonable steps to give notice of collection at or before the time of collection or, if that is not practicable, as soon as practicable after collection.

Recommendation 19: Further consideration should be given to the recommendations of the Commonwealth Privacy Act Review in relation to whether the PIPA requirements relating to collection notices should be amended to:

- require that collection notices should be clear and understandable (including where addressed to a child) and accessible; and
- require that collection notices contain additional details, such as details of the circumstances of handling where a high-risk activity is involved, information about the privacy policy and what it contains, and information about individual rights and types of information that may be disclosed to cross-border recipients.

Recommendation 20: PIPP 1 should be amended to enable personal information custodians to collect personal information about an individual from a person other than the individual, where the individual has consented or the custodian is required by law to collect the information.

Recommendation 21: The PIPA should be amended to insert a definition of 'consent' consistent with the definition of valid consent in the OAIC Guidelines on the Australian Privacy Principles.

Recommendation 22: Guidance on the design of consent requests for online services should be available to personal information custodians.

Recommendation 23: PIPP 1 should be amended to specify how personal information custodians should respond to receiving unsolicited information.

Recommendation 24: Further consideration should be given to aligning the PIPA with the Privacy Act in relation to cross-border in terms of:

- whether personal information custodians should be required to hold a reasonable belief that there are mechanisms for the individual to enforce existing privacy protections prior to cross-border disclosure;
- whether personal information custodians should be required to expressly inform individuals that, if the individual consents to cross-border disclosure, the custodian will not be obliged to take reasonable steps to ensure the recipient does not breach the PIPP (and, per the Privacy Act Review's further proposal, that privacy protections may not apply to the recipient); and
- whether personal information custodians retain responsibility for breaches of the PIPPs after they have taken reasonable steps to ensure the recipient deals with the information consistently with the PIPPs.

Recommendation 25: The PIPA should be amended to include a definition of 'disclosure' consistent with the current definition in the OAIC Guidelines on the Australian Privacy Principles.

Recommendation 26: The PIPA should be amended to require that collection, use, and disclosure of personal information must be fair and reasonable in the circumstances, in line with the recommendation of the Privacy Act Review.[557]

Recommendation 27: The PIPA (PIPP 1) should be amended to require personal information custodians to determine and record the purposes of collection, use, and disclosure of personal information, including any secondary uses or disclosures.

Recommendation 28: The scope of PIPA information handling exceptions relating to requirement or authorisation under law should be clarified.

Recommendation 29: The PIPA should be amended to state that consent to personal information handling must be 'voluntary, informed, current, specific, and unambiguous', in line with the proposal of the Privacy Act Review

Recommendation 30: The Tasmanian Government should participate in cross-jurisdictional work on the scope and harmonisation of research exceptions in privacy legislation (as proposed by the Privacy Act Review), including in relation to the introduction of a 'broad consent' option for research-related personal information handling.

Recommendation 31: Further consultation with stakeholders, including children and young people and their parents and carers, should be undertaken to ensure that privacy protections under the PIPA are appropriate for children and young people and are consistent with contemporary understandings of children's decision-making capacity. Matters for consultation may include:

- whether the PIPA should be amended to specify that consent to information handling will only be valid where the individual has capacity to consent;
- whether the PIPA should be amended to establish exceptions to consent requirements where seeking consent from a parent or guardian would be inappropriate or harmful for the child or young person; and
- whether guidance should be developed to assist personal information custodians to assess the capacity of children and young people on a case-by-case basis.

Recommendation 32: Guidance on capacity and consent, including guidance on recognising and facilitating supported decision-making, should be available to personal information custodians.

Recommendation 33: An individual 'right to object', with the same features as the right proposed by the Commonwealth Privacy Act Review, should be introduced in the PIPA.

[557] Privacy Act Review Report 2022 Proposals 12.1, 12.2, 12.3. See [5.4.24]–[5.4.26] above.

Part 6

Aligning the Personal Information Protection Principles with the Commonwealth Act: Data Quality, Data Security and Access and Correction

6.1 Overview of this Part

6.1.1 Data privacy legislation in Tasmania and other Australian jurisdictions imposes obligations on regulated bodies in relation to the quality of data (in terms of its accuracy, currency, and other features) and the security and protection of data. Legislation also enables individuals to access and correct personal information about them in certain circumstances.

6.1.2 This Part continues the TLRI's consideration of the similarities and differences between the Personal Information Protection Principles ('PIPPs') and the Australian Privacy Principles ('APPs') (defined at [2.5]) relating to data quality, data security, and access and correction, and the need for reform to the PIPPs arising from inconsistencies or other concerns with the adequacy of the Tasmanian protections.

6.2 The Tasmanian position

Data quality

6.2.1 Under the *Personal Information Protection Act 2004* (Tas) ('PIPA'), PIPP 3 obliges personal information custodians to take reasonable steps to ensure that, having regard to the purpose for which it is to be used, the personal information the custodian collects, uses, holds, or discloses is accurate, complete, up-to-date, and relevant to its functions or activities.

Data security

6.2.2 PIPP 4 requires a custodian to take reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification, or disclosure.[558]

6.2.3 PIPP 4 also specifies that a personal information custodian must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose, subject to any necessary approval from the State Archivist under the *Archives Act 1983* (Tas).[559]

[558] PIPP 4(1).
[559] PIPPs 4(2), 4(3).

Access and correction

6.2.4 PIPP 6 allows—but does not require—a personal information custodian to provide access to personal information it holds upon request from the person concerned.[560]

6.2.5 If a personal information custodian refuses such a request or does not respond to a request within 20working days, and the individual makes a further written request for access, the custodian must provide access 'as if … the written request were an application for assessed disclosure of information under Section 13 of the *Right to Information Act 2009* (Tas)' and the custodian were subject to that Act.[561]

6.2.6 Under PIPP 6(2), a person can request their information be amended, if it is incorrect, incomplete, out of date, or misleading, in accordance with the provisions in Part 3A of the PIPA. Part 3A addresses matters such as when a person may request amendment of information, the form that such a request must take, how the personal information custodian can amend information, and what the personal information custodian must do if it refuses a request to amend information.[562]

6.2.7 Following receipt of an information amendment request in the appropriate form,[563] a personal information custodian may amend the information by altering it or adding an appropriate notation to it.[564] While the amendment may be in the form of a notation to the original document, amendments that delete or expunge information which has been amended, or which destroy the document, cannot be made unless the State Archivist agrees.[565]

6.2.8 The personal information custodian must take all reasonable steps to notify the person of the decision on their information amendment request as soon as practicable, and no later than 20 working days after receipt of the request. Notice of a decision not to amend the information in the way requested must be in writing and state the reasons, name, and designation of the decision-maker, as well as information about the requester's right to make a complaint to the Ombudsman.[566]

6.2.9 If the personal information custodian refuses to amend the information following a request, the requester may give written notice, at any time, requiring the custodian to add a notation to the information which specifies the respects in which the information is claimed to be incomplete, incorrect, out of date, or misleading and (if applicable) setting out the information the requester claims is required to bring the information up to date.[567] The custodian must subsequently notify any person to whom the affected information is disclosed about the requester's claims about the information, the particulars of the notation, and, if the custodian considers it appropriate, reasons the custodian did not amend the information.[568]

[560] PIPP 6(1)(a).
[561] PIPP 6(1)(b).
[562] PIPA ss 17A, 17B.
[563] PIPA ss 17A, 17B.
[564] PIPA s 17C. According to s 17D, the notation must 'specify the way in which the information is incomplete, incorrect, out of date or misleading' and, 'if the information is claimed to be out of date, set out the information required to bring it up to date'.
[565] PIPA s 17I.
[566] PIPA s 17F.
[567] PIPA s 17G.
[568] PIPA s 17H.

6.3 The position in other jurisdictions

Data quality

6.3.1 PIPP 3 is substantially similar to APP 10 in the Commonwealth *Privacy Act 1988* (Cth) ('Privacy Act') in relation to entities' obligations relating to data quality, although:

- APP 10 only obliges responsible entities to take 'such steps (if any) as are reasonable in the circumstances' to ensure personal information it collects, uses, or discloses is accurate, up-to-date, complete, and relevant, rather than the 'reasonable steps' required under PIPP 3; and
- APP 10 only applies to the collection, use, and disclosure of information, while PIPP 3 extends further to information held by a personal information custodian.[569]

6.3.2 Other jurisdictions also have provisions about data quality relating to the requirement to take reasonable steps to ensure that the information that is collected, used, or disclosure is accurate, complete, and up to date.[570]

Data security

6.3.3 The Privacy Act's APP 11 addresses the security of personal information. It imposes similar security obligations to PIPP 4 in the PIPA. Other jurisdictions also have provisions that address data security.[571]

6.3.4 APP 11.1 obliges APP entities to 'take such steps as are reasonable in the circumstances' to protect information from misuse, interference, and loss, and from unauthorised access, modification, or disclosure.[572] This is also the position in New South Wales, Queensland, the ACT, and the Northern Territory.[573] In contrast, PIPP 4 does not require regulated entities to take steps to protect information from interference.

6.3.5 Under APP 11.2, APP entities also have an obligation to take reasonable steps to destroy or de-identify information applies where the information is:

- no longer needed by an entity for any purpose 'for which the information may be used or disclosed by the entity under' the APPs; and

[569] Other APPs apply to information that an APP entity holds (such as APP 11 regarding security of information). The *Privacy Act 1988* (Cth) defines 'holds' to mean 'the entity has possession or control of a record that contains the personal information' (s 6(1) definition of 'holds'). The PIPA does not define the term 'holds'.
[570] PPIP Act (NSW) s 11, 16; PDP Act (Vic) IPP 3; IP Act (Qld) IPPs 3, 8; IPA (ACT) TPP 10; *Information Act* (NT) IPP 3. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[571] PPIP Act (NSW) s 12; PDP Act (Vic) IPP 4; IP Act (Qld) IPP 4; IP Act (ACT) TPP 11; *Information Act* (NT) IPP 4. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[572] APP 11.1.
[573] PPIP Act (NSW) s 12; PDP Act (Vic) IPP 4; IP Act (Qld) IPP 4; IP Act (ACT) TPP 11; *Information Act* (NT) IPP 4. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.

- not contained in a Commonwealth record or required under an Australian law or court/tribunal order to be retained.[574]

6.3.6 Provisions relating to the de-identification or destruction of information also exist in other jurisdictions.[575]

6.3.7 The Privacy Act also obliges APP entities to investigate and report certain data breaches involving unauthorised access to, disclosure of, or loss of personal information. The data breach notification scheme is discussed in [8.12.1] of this Report.

6.3.8 The European Union's *General Data Protection Regulation 2016/679* ('GDPR') serves as a useful further point of comparison because it provides greater detail than the PIPA and Privacy Act principles on data security. Whereas Australian laws simply require entities to take 'reasonable steps' to protect the security of personal information, Article 32 of the GDPR provides for specific measures that should be taken to achieve such security. These include provisions relating to:

- the pseudonymisation (see above at [4.2.13]) and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability, and resilience of systems and services that process the information;
- the ability to restore the availability of, and access to, personal data in a timely manner in the event of a physical or technical incident; and
- a process for regularly testing, assessing, and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

6.3.9 The GDPR also allows entities to demonstrate compliance through adherence to an approved code of conduct or certification scheme.

6.3.10 Article 17 of the GDPR also provides for a 'right to be forgotten'—also known as a right to erasure —in some circumstances. Where this GDPR right applies, it requires data controllers to erase personal information without delay if requested by the individual, and to take reasonable steps to inform other controllers.

6.3.11 The GDPR right applies where either:

- retaining the information is no longer necessary in relation to the purposes for which it was collected;
- the request to erase the information amounts to a withdrawal of the consent that allowed the information to be collected or used in the first place;
- the individual objects to the use under the right to object (as described at [5.4.40] and following);
- the information was collected through use of an online service by a child, including where the parent or guardian consented; or
- the information was collected, used, disclosed, or otherwise handled in an unlawful way.

[574] APP 11.2

[575] PPIP Act (NSW) s 12; PDP Act (Vic) IPP 4IP Act (ACT) TPP 11; *Information Act* (NT) IPP 4. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.

6.3.12 There are various exceptions where the information is nevertheless able to be retained, including where retention is necessary:

- for the exercise of the right to free expression;
- for compliance with legal obligations or defence of legal claims;
- for reasons of public interest in the area of public health; or
- to allow archiving that is otherwise authorised in the public interest, for scientific or historical research purposes, or for statistical purposes.[576]

Access and correction

6.3.13 Under Commonwealth law, APP 12 addresses access to personal information; APP 13 addresses correction of personal information. These principles contain similar provisions to PIPP 6 and Part 3A of the PIPA (described above at [6.2.6] and following). Access and correction are also addressed in other jurisdictions.[577] APP 12 and 13 deal with the following matters.

- *Obligation to provide access:* APP 12 is imperative, stating that an APP entity 'must, on request by the individual, give the individual access to the information', with specified exceptions applying to agencies where required or authorised under freedom of information legislation or other laws.[578] This is in contrast to the permissive phrasing of PIPP 6, which states that a custodian 'may provide' access and does not discuss qualifications or exceptions.
- *Time limits:* Under APPs 12 and 13, requests to access or correct personal information must be handled within 30 days, in contrast to the 20-working-day limit under PIPP 6.[579]
- *Notice of refusal to give access:* Under APP 12, if an agency has refused to give access under one of the specific exceptions, it must give the requester written notice of the reasons for the refusal (except where it would be unreasonable to do so), the mechanisms to complain about the refusal, and other matters prescribed by regulations. There is no such notice requirement in the PIPA[580].
- *Access charge:* APPs 12 and 13 expressly provide that an agency cannot charge an individual for access to their information, for requesting a correction, for making a correction, or for

[576] See GDPR art 89 in relation to the requirements for archiving purposes.
[577] PPIP Act (NSW) s 14, 15; PDP Act (Vic) IPP 6; IP Act (Qld) IPPs 6, 7; IP Act (ACT) TPP 12; *Information Act* (NT) IPP 3. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[578] APPs 12.1, 12.2. Imperative phrasing is also used in NSW, Victoria, Queensland, the ACT, and the NT (subject to the exemptions set out the respective legislation) (PPIP Act (NSW) s 14, 15; PDP Act (Vic) IPP 6; IP Act (Qld) IPPs 6, 7; IP Act (ACT) TPP 12; *Information Act* (NT) IPP 6. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP. Different exceptions apply to organisations; they will not be required to provide access in circumstances such as where doing so would pose a serious threat to life, health, or safety of an individual or public health or safety; where the request is frivolous or vexatious; where giving access would be unlawful; and where the entity suspects unlawful activity or serious misconduct and giving access would be likely to prejudice the taking of appropriate action, among others: APP 12.3.
[579] PIPA s 17E.
[580] APP 12.9. Provisions in relation to notice relating to access also exist in Victoria (IPP 6); ACT (TPP 12), NT (IPP 6). It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.

associating a statement (described below).[581] The PIPA does not mention charges in relation to access or correction of information.

- *Grounds for correction:* APP 13 creates the same grounds for correction as the PIPA (namely, where information is inaccurate, out-of-date, incomplete, or misleading) and an additional ground allowing information to be corrected where it is 'irrelevant'.[582] It specifies that an entity must take reasonable steps in the circumstances (if any) to correct information where either the entity is satisfied it meets one of these grounds, or where the individual requests correction.[583] In either of these circumstances, the entity must take reasonable steps (if any) to correct the information to ensure that, having regard to the purpose for which it is held, is accurate, up-to-date, complete, relevant, and not misleading.[584]
- *Request for notation following refusal to correct:* APP 13 enables an individual whose request to correct information has been refused to subsequently request the entity associate with the information a statement that the information is inaccurate, out-of-date, incomplete, irrelevant, or misleading. The entity is required to 'take such steps as are reasonable in the circumstances to associate the statement in such a way as to make the statement apparent to users of the information'.[585] This phrasing differs from the corresponding PIPA provisions, which state that the requester may 'require' the notation and that custodians 'must' notify subsequent recipients of the information of the notation.[586]
- *Notice to third parties of prior disclosure:* Under APP 13, in circumstances where an individual's personal information has previously been disclosed by one entity to another entity, the individual can request that the entity notify the other entity of the correction.[587] Reasonable steps must be taken to comply with this request, unless doing so would be impracticable or unlawful.[588] PIPP 6 and Part 3A of the PIPA only require custodians to notify persons to whom the information is disclosed about a notation added to the information under Section 17G, where a request for correction has been refused.[589]

6.3.14 Under the Privacy Act, only personal information that the entity 'holds' may be accessed and corrected.[590] This means that information published on social media falls outside the operation of the APPs. The Office of the Australian Information Commissioner ('OAIC') has stated that such information is no longer within an agency's possession or control and is therefore not 'held' by that agency.[591] This is in contrast to the GDPR right to rectify inaccurate data, which applies even where the

[581] APPs 12.7, 13.5. Note that the *Freedom of Information Act 1982* (Cth) also provides a right to access and correct personal information held by Commonwealth agencies and public authorities or official documents of Ministers, with internal and external review of decisions available. This is also the position in the ACT TPP 12.7 in relation to making a request or access to personal information, and 13.5 in relation to request to correct personal information.
[582] APP 13.1. NSW, Queensland, and the ACT also contain a reference to the relevance of the information: PPIP Act (NSW) s 15(1); IP Act (Qld) IPP 7(1); IP Act (ACT) 13.1. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[583] APP 13.1(b). The PIPA does not draw this distinction and simply states that a person may request correction of information 'if it is incorrect, incomplete, out of date or misleading': s 17A.
[584] *Privacy Act 1988* (Cth) sch 1, APP 13.1.
[585] APP 13.4. See also PPIP Act (NSW) s 15(3); PDP Act (Vic) IPP 6.6; IP Act (Qld) IPP 7(4); IP Act (ACT) 13.4. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[586] PIPA ss 17G, 17H.
[587] This is also the case in the ACT: IP Act (ACT) 13.2. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[588] PIPA sch 1, APP 13.2.
[589] PIPA s 17H.
[590] APP 12.1, APP 13.1(a).
[591] OAIC, *Submission to Privacy Act Review* 51.

personal data is publicly available. In Article 5(1)(d) of the GDPR, the 'accuracy principle' requires information to be accurate and up to date, and mandates that reasonable steps must be taken to rectify or erase inaccurate data.

6.3.15 The GDPR also establishes a 'right for individuals to confirm whether or not personal data concerning them are being processed, and, where that is the case, access to the personal data', as well as information such as the purposes of the processing, categories of personal data concerned, and recipients or categories of recipient to whom the personal data have been, or will be, disclosed, among others.[592]

6.4 Proposals in the Commonwealth Privacy Act Review

6.4.1 The Privacy Act Review Final Report proposed the introduction to the Commonwealth legislation of a set of individual rights relating to data quality, security, access, and correction. The Review argued that these rights would enhance transparency and control over individuals' privacy and strike a better balance between the protection of individuals' privacy and the interests of entities 'in carrying out their functions and activities' than the existing legislation.[593] It also recommended the introduction of some specific and general exceptions to these new rights.

6.4.2 The Review proposed that the individual privacy rights should be situated within a regulatory framework that enables APP entities and individuals to work together to determine the best resolution for individuals' concerns, which may include finding the most appropriate right or combination of rights, rather than insisting on strict compliance with each right in all cases.[594]

6.4.3 The Review proposed the introduction of five individual rights. These include, first, three individual rights 'directed at giving individuals more control over their information' relating to data security, access, and correction:

- a **right to erasure:** 'a right to have information deleted' (discussed at [6.4.5] below);
- a **right to correction:** 'a right to require that information be accurate, up-to-date, complete; relevant and not misleading' (discussed at [6.4.19] below); and
- a **right to de-index** certain search results: 'a narrow right to have internet search results about an individual de-indexed in specific circumstances' (discussed at [6.4.8] below).[595]

6.4.4 Second, the Review proposed that the Privacy Act be amended to create two rights to improve transparency:

- a **right to access and explanation:** 'a right to know what personal information is held, where it came from, and what is being done with it (including meaningful information about how automated decisions using an individual's personal information are made (see [7.37]); this right is discussed at [6.4.15] below;[596] and
- a **right to object** to the collection, use, and disclosure of personal information (discussed at 5.4.40] above).[597]

[592] GDPR art 15(1).
[593] Privacy Act Review Report 2022 167.
[594] Ibid.
[595] Privacy Act Review Report 2022 165.
[596] Ibid 166.
[597] Ibid.

Data security

6.4.5 The Review recommended that a legislated **right to erasure** should have three features:

- individuals should be able to assert the right in relation to any of their personal information;
- where there has been an erasure request, APP entities who collected the personal information from, or disclosed it to, a third party must inform the individual about the third party and notify the third party of the request (except where this is impossible or involves disproportionate effort);[598] and
- certain limited information (such as joint personal information, metadata, financial records, and rental or property records) should be quarantined rather than erased on request, to ensure it is available for law enforcement purposes and that the right is not exploited by those seeking to conceal criminal activity.[599]

6.4.6 The Review noted concerns expressed by 'a large number and broad range of submitters' about the effect of this right on APP entities' activities in the public interest and suggested that there be further stakeholder engagement on the detail of exceptions.[600]

6.4.7 The Final Report characterised the right to erasure as 'effectively … an extension of APP 11.2 by requiring the entity to destroy the information upon request of the individual, rather than at the time the entity considers this is required'.[601] The Commonwealth Government agreed in-principle with this proposal.[602]

6.4.8 The right to **de-index search results** was characterised as 'a sub-category of erasure'.[603] The Review proposed the creation of a right, assertable against search engines, for search results containing personal information to be de-indexed, meaning they would not be listed in search results, regardless of whether the information continues to be published lawfully elsewhere online. As explained in the Report:

> The content remains at its source on the internet. The right regulates the ease of access to personal information through a search engine, not its removal from the internet.[604]

6.4.9 The Review recommended that, in keeping with similar grounds applying under the GDPR, the right to de-index search results should apply to personal information which is: sensitive information; information about a child; excessively detailed (such as home address or personal phone number); or

[598] The Privacy Act Review noted in the final report that this would be similar to Article 19 of the GDPR: Privacy Act Review Report 2022 176.
[599] Privacy Act Review Report 2022 Proposal 18.3 and 174–176.
[600] Ibid 175.
[601] Ibid 174. This was broadly consistent with the recommendation in the ACCC's *Digital Platforms Inquiry* that Australia adopt a right to erasure, subject to possible further qualifications. For example, exceptions that allow the retention of information where it is necessary for the performance of a contract to which the consumer is a party, is required by law, or is otherwise necessary for an overriding public reason: ACCC, *Digital Platforms Inquiry* 473.
[602] Government Response 18.
[603] Privacy Act Review Report 2022 177.
[604] Ibid 178.

inaccurate, out-of-date, incomplete, irrelevant, or misleading.[605] The Commonwealth Government agreed in-principle with this proposal.[606]

6.4.10 A chapter of the Privacy Act Review Final Report was dedicated to security, destruction, and retention of personal information.[607] The Review proposed some amendments to APP 11 relating to security measures, including amending APP 11 to:

- state in APP 11.1 that the 'reasonable steps' APP entities must take to protect information include technical security measures and organisational measures (such as those relating to governance, internal practices, processes, and systems), on the basis that this would improve certainty and understanding of what reasonable steps are required.[608] The Government agreed with this proposal.[609]
- include a 'set of baseline privacy outcomes' that APP entities would need to ensure their practices enable them to meet, developed in consultation with industry and government.[610] The Government agreed in-principle with this proposal.[611]
- require APP entities to establish and periodically review maximum and minimum retention periods for personal information which take into account: the type, sensitivity, and purpose of the information; the entity's organisational needs; and any obligations entities have under other legal frameworks.[612] The Government agreed in-principle with this proposal.[613]

6.4.11 The Review also proposed amendments to APP 11.1 to improve the security of de-identified information by obliging APP entities to take reasonable steps to protect de-identified information from misuse, interference, and loss, and from unauthorised re-identification, access, modification, or disclosure.[614] The Government noted these proposals and undertook to further consider how the policy intent of protecting against re-identification risks could be achieved.[615]

6.4.12 The Review further recommended changes to the regulation of the destruction and de-identification of personal information by improving OAIC guidance on APP 11 to clarify what reasonable steps may be undertaken to destroy or de-identify personal information, which could provide tailored guidance for 'specific industry, method of destruction and/or the type or sensitivity of the information'.[616] The Government agreed with this proposal.[617]

6.4.13 In light of the range of retention requirements imposed on APP entities in Australian laws other than the Privacy Act, and the changed risk landscape in the digital era, the Review proposed a separate Commonwealth review of 'all legal provisions that require retention of personal information' to ensure there is an appropriate balance between policy objectives and privacy and cyber security risks

[605] Privacy Act Review Report 2022 Proposal 18.5 and 178–179. The Review recommended this right be jurisdictionally limited to Australia, and that '[t]he search engine may refer a suitable request to the OAIC for a fee': ibid.
[606] Government Response 18.
[607] Privacy Act Review Report 2022 ch 21.
[608] Ibid Proposal 21.1 and 222.
[609] Government Response 8.
[610] Privacy Act Review Report 2022 Proposal 21.2 and 223. The Review suggested the outcomes-based factors in art 32(1) of the GDPR and the Australian Cyber Security Centre's Cyber Security Principles could be used as a starting point for this: Privacy Act Review Report 2022 224.
[611] Government Response 8
[612] Privacy Act Review Report 2022 Proposal 21.7 and 228.
[613] Government Response 9.
[614] Privacy Act Review Report 2022 Proposal 4.6(a).
[615] Government Response 5, 9.
[616] Privacy Act Review Report 2022 Proposal 21.5 and 226.
[617] Government Response 8.

of entities holding significant volumes of personal information, the scope and scale of which should be determined in consultation with the States and Territories.[618] The Government agreed in-principle with this proposal.[619]

6.4.14 The Review also considered the adequacy of the Privacy Act's notification of data breaches scheme. This is discussed at [8.13] of this Report.

Access and correction

6.4.15 The Privacy Act Review recommended the introduction of a **right to access and explanation**, which expands on the existing right of access in APP 12.[620]

6.4.16 The Final Report argued that a broader right of explanation than currently existed would be appropriate in order to enhance transparency and ensure that individuals can exercise their other rights. This would also be consistent with regulation in Europe (via the GDPR), Canada, Singapore, and California.[621] The Review characterised this as complementary to the enhanced collection notice requirements proposed elsewhere in its Report (discussed at [7.3], below).[622]

6.4.17 The Review proposed that the right to access in APP 12 be retained, and that it be augmented with the following additional features:

- 'an APP entity must identify the source of the personal information it has collected indirectly, on request by the individual';
- 'an APP entity must provide an explanation or summary of what it has done with the personal information, on request by the individual'; and
- 'the entity may consult with the individual about the format for responding to a request, and the format should reflect the underlying purpose of ensuring the individual is informed, as far as is reasonable, about what is being done with their information'.[623]

6.4.18 The Government agreed in-principle with this recommendation.[624]

6.4.19 The Privacy Act Review's recommendation in relation to a **right to correction** entailed extending the existing right (which is available when information is inaccurate, out-of-date, incomplete, irrelevant, or misleading) to generally available publications online over which the APP entity maintains control, such as webpages.[625] The Government agreed in-principle with this proposal.[626]

General exceptions to individual rights

6.4.20 The Privacy Act Review recommended that general exceptions should apply to all five of the proposed individual rights in three circumstances:

---

[618] Privacy Act Review Report 2022 Proposal 21.6 and 226–267.
[619] Government Response 9.
[620] Privacy Act Review Report 2022 Proposal 18.1.
[621] Ibid 168–169.
[622] Ibid.
[623] Privacy Act Review Report 2022 Proposal 18.1 and 172. The Review also proposed that organisations (but not government agencies and related bodies) be permitted to charge a nominal fee for access and explanation.
[624] Government Response 18.
[625] Privacy Act Review Report 2022 Proposal 18.4.
[626] Government Response 18.

- where there are competing public interests;
- where required or authorised by law and legal relationships; and
- where technically infeasible or an abuse of process.[627]

6.4.21 The Government agreed in-principle with these proposed exceptions.[628]

6.4.22 The competing public interests exception would apply where 'the public interest in a particular activity outweighed the public interest in protecting privacy', the assessment of which would involve an evaluative, balancing exercise.[629] Where the exception was found to apply, the Review recommended that rights should 'continue to operate to the extent the balancing does not weigh against it'.[630]

6.4.23 The Review considered that the public interest exception should include an exception for freedom of expression, an exception where compliance would impact law enforcement, exceptions regarding health care and research, and exceptions concerning national security and missing persons.[631]

6.4.24 The second general exception to individual rights, which would apply where required or authorised by law or where compliance would be unlawful, was intended to address relationships with a legal character and to:

- ensure the rights cannot be exercised contrary to law, or displace obligations under other regulatory regimes; and
- ensure the rights do not interfere with the performance of contractual or other like obligations.[632]

6.4.25 The third exception, relating to technical infeasibility or abuse of process, was proposed in contemplation of circumstances where:

- technical limitations on how information is held or used, or the nature of the request and the information, would make actioning the request unreasonable; and
- requests are frivolous or vexatious (which would be an extension of the similar exception already applying to access in APP 12.3).[633]

Assisting and responding to the exercise of individual rights

6.4.26 The Privacy Act Review also proposed that APP entities should meet certain requirements when responding to the exercise of one or more of the proposed individual rights. The Review suggested these requirements would have several purposes, including: 'address[ing] the imbalance in understanding between the APP entity and the individual, whilst facilitating the relationship between the parties'; balancing the enjoyment of individual rights with the administrative burden on APP entities; and supporting compliance by setting standards and providing guidance.[634]

6.4.27 The Review recommended that APP entities should be required to:

[627] Privacy Act Review Report 2022 Proposal 18.6.
[628] Government Response 18.
[629] Privacy Act Review Report 2022 180.
[630] Ibid.
[631] Ibid 180–181.
[632] Ibid Proposal 18.6 and 181–182.
[633] Ibid Proposal 18.6 and 181.
[634] Privacy Act Review Report 2022 184–187.

- provide 'reasonable assistance' to individuals in exercising their rights (in order to avoid APP entities taking 'a technical or legalistic approach to the wording of a request, which may not be in the interests of either party'), which was modelled on a similar requirement in freedom of information legislation;[635]
- take 'reasonable steps to respond to an exercise' of an individual right, including ensuring that a refusal of a request is accompanied by an explanation and information about how an individual can lodge a complaint;[636] and
- 'acknowledge receipt of a request to exercise an individual right within a reasonable time and provide a timeframe for responding', with the default timeframe of 30 days for agencies.[637]

6.4.28 The Government agreed in-principle with these recommendations.[638]

6.5 Consultation

6.5.1 The TLRI Issues Paper contained several questions relating to data quality, security, and/or access and correction:

> Are there any other amendments to the PIPPs that you think should be made?[639]
>
> Should any of the other potential reforms be introduced, including:
>
> … a right to be forgotten[640]

Data security

6.5.2 Dr Joel Scanlan expressed support for the introduction of a 'right to be forgotten'. Dr Scanlan also observed that the deletion of old data is costly.[641]

6.5.3 As discussed in [4.4.4], academics in the Centre for Law and Genetics at the University of Tasmania (Professor Margaret Otlowski, Emeritus Distinguished Professor Dianne Nicol, and Dr Lisa Eckstein) recommended that Tasmania follow the Privacy Act Review's proposals to extend protections to de-identified information that are proportionate to the risk of the information being re-identified.

6.5.4 Richard Griggs proposed that PIPP 4(2) should be amended to make destruction or permanent de-identification of personal information that is no longer needed for any purpose *mandatory*, replacing the current requirement that custodians take 'reasonable steps'.

Access and correction

6.5.5 Two submitters raised concerns about the operation of PIPP 6 in relation to access to personal information.

[635] Privacy Act Review Report 2022 Proposal 18.8 and 184.
[636] Ibid Proposal 18.9.
[637] Ibid Proposal 18.10.
[638] Government Response 18.
[639] Issues Paper Part 2, Question 2.8.
[640] Ibid Part 2, Question 2.9(c).
[641] Submission 20 (Dr Joel Scanlan).

6.5.6 The Tasmanian Ombudsman expressed concern about the problematic interaction between the PIPA and the *Right to Information Act 2009* (Tas) ('RTI Act') in the application of PIPP 6, which requires personal information custodians to treat further written requests for access (where the original request was refused or not responded to within 20 working days) 'as if … the written request were an application for assessed disclosure of information' under Section 13 of RTI Act (see [6.2.5] above).[642]

6.5.7 According to the Tasmanian Ombudsman:

> The use of the phrase 'as if' [in PIPP 6(1)(b)] creates difficulty because it is not a deeming provision; it does not render a request under this provision an application under the RTI Act. A literal interpretation of the provision requires the personal information custodian to determine the matter in the same manner and having regard to the same principles as an application under section 13 of the RTI Act, but does not import the other provisions of the RTI Act. This means there are no review rights nor prescribed timeframes which, in a practical sense, leave applicants who have gone down the [PIPA] access path with no ability to seek external review of a failure to provide access or redress in respect of delay.

6.5.8 The Ombudsman suggested that amendments to both the RTI Act and the PIPA would be necessary to address this issue.

6.5.9 Alex Kendall of Phillips Taglieri Barristers & Solicitors similarly argued that the wording of PIPP 6(1)(b) produced confusion about the interaction between the PIPA and the RTI Act, particularly in terms of whether the offence in Section 50 of the RTI Act for failure to disclose information applies to requests made under the PIPA.

6.5.10 Mr Kendall submitted that the current wording of the PIPA in this and other respects makes it difficult for lawyers to obtain their clients' personal information, even with express written consent. Mr Kendall submitted that personal information custodians refuse access 'on the basis of various excuses' involving misconstructions or misapplications of the PIPPs.

6.5.11 On this basis, Mr Kendall suggested that PIPP 6 should be amended to provide individuals with unrestricted access to their personal information by:

- replacing 'may provide that individual with access to his or her personal information' with 'must provide that individual with access to his or her personal information' in PIPP 6(1)(a), to clarify that personal information custodians must disclose information on request;
- deleting paragraph (b) of PIPP 6(1);
- imposing a requirement for personal information custodians to provide copies (rather than merely 'access') to the personal information; and
- prescribing a fee for access and copies (in order to avoid personal information custodians 'quoting excessive amounts'—with Phillips Taglieri indicating experience of fees ranging from $50 to over $1,000).[643]

6.5.12 The Tasmanian Ombudsman also described as 'somewhat curious' Part 3A of the PIPA—specifically, the provision that enables a person to 'require' a personal information custodian to add a notation to information where the custodian has refused a request to amend information that the person

[642] PIPP 6(1)(b).
[643] Submission 1 (Alex Kendall).

considers is incorrect, incomplete, out-of-date, or misleading (described above at paragraph [6.2.5]). The Ombudsman observed that the PIPA neither permits custodians to refuse to add such a notation nor imposes any qualifications or limitations on the information that must be included (except insofar as it is limited to information related to personal information, and that it must specify the basis of the person's claim and, if applicable, set out the information claimed to be necessary to bring it up to date).[644] The Ombudsman described this as 'problematic in practice' because some 'persistent and inflexible applicants' utilise the provision in a manner that consumes considerable resources.[645]

6.5.13 Several submissions also raised the possibility of the introduction of a data breach notification scheme under the PIPA. These are discussed at [8.14] below.

6.6 The TLRI's view

Data quality

6.6.1 The TLRI observes that the scope of PIPP 3 is wider than the scope of APP 10 (the APP equivalent) because it applies to information held by a personal information custodian. Having neither sought nor received submissions on this point, the TLRI makes no recommendations in relation to it.

Data security

6.6.2 Data security was identified in some submissions to this project and in the Privacy Act Review as a matter of concern, especially in light of developments in overseas jurisdictions, changed community expectation, and increased risks associated with digital platforms' collection and use of data.[646]

6.6.3 The TLRI observes that PIPP 4 is slightly narrower than APP 11.1, in that it does not place obligations on custodians to take steps to protect information from 'interference'. It is unclear whether this omission has significant consequences for data security in Tasmania; submissions were not sought or received on this point.

6.6.4 The TLRI notes that the Privacy Act Review recommendations to amend APP 11 to increase the level of detail and guidance on the steps that regulated entities must take, and baseline privacy outcomes these steps should enable them to meet, to protect personal information could bring Australian regulation more closely into line with regulation overseas. The TLRI notes that the Commonwealth Government agreed, or agreed in-principle, with these proposals. The TLRI recommends that corresponding amendments to PIPP 4 would also enhance both consistency across jurisdictions and the adequacy of data security measures in Tasmania.

6.6.5 The TLRI notes that the submission to this review by Richard Griggs,[647] and submissions to the equivalent Commonwealth review, were critical of the 'overly permissive nature' of destruction and de-identification requirements,[648] which require regulated entities to take reasonable steps to destroy or de-identify information that is no longer needed.

[644] See PIPA s 17G.
[645] Submission 4 (Tasmanian Ombudsman).
[646] See, eg, Privacy Act Review Report 2022 167.
[647] Submission 10 (Richard Griggs).
[648] See Privacy Act Review Report 2022 226.

6.6.6 The TLRI observes that the Privacy Act Review did not propose any amendments to APP 11 to strengthen these requirements at the Commonwealth level. It did propose (and the Commonwealth Government accepted) that the OAIC should develop more detailed and tailored guidance on what constitutes reasonable steps in this regard. In the TLRI's view, the development of such guidance (or equivalent, Tasmania-specific guidance) could assist personal information custodians to meet their obligations under PIPP 4.

6.6.7 The TLRI also notes the Privacy Act Review proposal that APP entities should be obliged to take steps to protect de-identified information from misuse, interference, and loss, and from unauthorised re-identification, access, modification; or disclosure,[649] although the Commonwealth Government merely noted this proposal (see [6.4.11] above).

6.6.8 The TLRI considers that the Privacy Act Review recommendation to introduce a qualified 'right to erasure' would also be appropriate for the PIPA because it would give Tasmanians greater control over their personal information.

6.6.9 The TLRI observes that the Privacy Act Review gave comprehensive consideration to the implications of this right for authorised archiving, law enforcement, and other purposes (such as the exercise of the right to free expression and public interest in the area of public health) and recommended appropriate exceptions or quarantining requirements to address such concerns.

6.6.10 The TLRI notes that, unlike the Privacy Act, the PIPA includes information about certain deceased persons within the definition of 'personal information' and empowers a deceased person's next-of-kin to exercise the deceased person's personal information rights.[650] Consideration of the availability and exercise of the right to erasure in relation to deceased persons—and the other individual rights recommended for introduction in this Report—including in terms of individuals' estate planning and the powers of executors, would be necessary prior to the introduction of the rights in the PIPA.

6.6.11 The TLRI also notes the Privacy Act Review's recommendation that all Commonwealth laws which require retention of personal information should be reviewed in light of growing cyber-security risks associated with entities holding large volumes of information (see paragraph [6.4.13] above). The TLRI notes that submissions to this review raised related concerns about data breaches (see Part 8 below). The TLRI recommends a similar review process be undertaken in Tasmania.

6.6.12 The TLRI considers that strengthened data breach notification measures should be implemented in Tasmania. This is discussed in more detail in Part 8 of this Final Report.

Access and correction

Access

6.6.13 The TLRI observes that the Commission of Inquiry into the Tasmanian Government's Responses to Child Sexual Abuse in Institutional Settings ('CoI') made a number of recommendations relating to access to information and records by victim-survivors of child sexual abuse under the PIPA and the RTI Act in its Final Report ('CoI Final Report'). These included a recommendation that the operation of the RTI Act and the PIPA be reviewed and reformed to 'ensure that people's rights to

[649] Privacy Act Review Report 2022 Proposal 4.6.
[650] PIPA ss 3 (definition of 'personal information'), 3A.

obtain information are observed in practice' and that 'access is as simple, efficient, transparent and trauma-informed as possible'.[651]

6.6.14 The CoI recommended that such a review should consider a range of reforms to the RTI Act and the PIPA, including reforms to:

- 'include an explicit presumption in favour of disclosure' in both Acts; and
- 'require that a personal information custodian under the *Personal Information Protection Act 2004* "must provide" rather than "may provide" personal information upon request from an individual who is the subject of that information, subject to any appropriate exemptions to that requirement'.[652]

6.6.15 Taking into consideration submissions received in response to the TLRI Issues Paper, the recommendations of the CoI, and the inconsistencies between the PIPA and the Commonwealth Privacy Act, the TLRI considers that it would be appropriate for PIPP 6 to be amended in several respects.

6.6.16 First, PIPP 6 should be amended to mirror APP 12 by requiring personal information custodians to:

- provide individuals with access to their personal information upon request;[653]
- provide access to requested personal information in the manner requested by the individual, as long as this is reasonable and practicable, without charge;[654]
- give written notice of the reasons for a refusal to give access and the mechanisms available to complain about the refusal (which are discussed further in Part 8 of this Report).[655]

6.6.17 The TLRI also recommends that, consistent with the CoI's Recommendation 17.8, PIPP 6 be amended to include an explicit presumption in favour of disclosure. In light of the Tasmanian Ombudsman's submission raising concerns about the possibility of misuse of access and correction rights, the TLRI considers that these reforms should be balanced against a need to provide protections against frivolous or vexatious requests.

6.6.18 The TLRI notes that the CoI also reported that Tasmanian public authorities have different processes and levels of resourcing for handling PIPA and RTI Act requests. It found that, generally, departments have dedicated teams to handle RTI Act requests but do not have centralised registers or designated staff appointed to deal with PIPA requests.[656] Evidence to the CoI raised concerns about the capacity of departments to handle and accurately respond to requests in a timely manner.[657]

6.6.19 The TLRI notes and supports the CoI's recommendation that '[t]he Tasmanian Government should consider centralising the management of access to information processes in a specialist unit or department, supported by access to information liaison officers located in government departments and

[651] Commission of Inquiry into the Tasmanian Government's Responses to Child Sexual Abuse (Report, August 2023) Recommendation 17.8(1) <https://www.commissionofinquiry.tas.gov.au/__data/assets/file/0011/724439/COI_Full-Report.pdf> ('CoI Final Report').
[652] Ibid Recommendation 17.8(2).
[653] APP 12.1
[654] APP 12.4(b). The TLRI observes that OAIC guidance gives examples of email, phone, in person, hard copy or electronic record access: OAIC, *APP Guidelines* [12.68].
[655] APP 12.9.
[656] CoI Final Report 190.
[657] Ibid 191.

agencies',[658] and that funding be provided to government departments, agencies, and the Ombudsman to ensure access requests are processed within statutory timeframes, to speed up external review of decisions, and provide trauma-informed training to the Tasmanian State Service in relation to victim-survivors' access to information.[659] The TLRI considers that these recommendations could benefit all persons whose information privacy is protected by the PIPA.

6.6.20 The TLRI considers that it would also be appropriate to amend PIPP 6 to introduce a right to explanation, consistent with the right to access and explanation proposed by the Commonwealth Privacy Act Review. This would augment the existing right to access by enabling individuals to request, in an appropriate format, explanations about the source of personal information that a custodian has collected indirectly, and explanations or summaries of what a custodian has done with personal information.[660]

6.6.21 The TLRI notes the criticisms by several submitters in response to the Issues Paper, including the Tasmanian Ombudsman, of the current process for requesting access to personal information in PIPP6. These criticisms focused on PIPP 6(1)(b) and argued that this provision creates two confusing and inconsistent pathways for requesting access to personal information. The TLRI notes that the CoI reported receiving similar submissions about the delays involved in the two-step PIPA process and recommended that consideration be given to reforming the PIPA and RTI Act to 'streamline the interface between [the Acts] to overcome what has, by default, become a two-step process to obtain personal information'.[661]

6.6.22 On this basis, the TLRI recommends this provision be amended to simplify the access process, including to address the current lack of clarity around the interaction of the PIPA and the RTI Act where a custodian has refused an access request or has failed to respond within 20 days. The adequacy of complaint and review mechanisms where access requests are refused is discussed further in Part 8 of this Report.

Correction

6.6.23 The TLRI considers that it would be appropriate to qualify the current entitlement in Section 17G of the PIPA for individuals to *require* that a custodian add a notation to information where the custodian has refused a request to amend the information. The TLRI considers that it would be more appropriate to express this as a right to *request* (for no charge) the addition of a notation, which the personal information custodian must take reasonable steps to associate with the information in a manner that makes it apparent to future users and to which the custodian must respond within 30 days. This would be consistent with many other obligations imposed on personal information custodians under the PIPPs and with the Commonwealth Privacy Act. If accompanied by appropriate complaint and review mechanisms (discussed in Part 8 of this report), this would appropriately balance individuals' rights with regulatory burden, addressing the concerns raised by the Tasmanian Ombudsman about use of this provision in a 'persistent and inflexible' manner that consumes considerable resources.[662]

6.6.24 The TLRI observes that the equivalent right to request association of a statement in the Privacy Act does not impose a requirement for APP entities to give written notice of a refusal. This is inconsistent with other elements of the principles relating to access and correction (see [6.3.13] above). In the TLRI's view, personal information custodians should be required to provide a written notice of

[658] CoI Final Report Recommendation 17.8(3).
[659] Ibid Recommendations 17.8(4) and 19.2.
[660] See Privacy Act Review Final Report 2022 Proposal 18.1.
[661] CoI Report Recommendation 17.8(2).
[662] Submission 4 (Tasmanian Ombudsman).

refusal to add a notation to personal information in order to support individuals to exercise their rights under the PIPA.

6.6.25 The TLRI also notes the Commonwealth Privacy Act Review recommended that the existing 'right to correction' in the Privacy Act (which is similar to the right in s 17A of the PIPA) be extended to generally available publications online over which APP entities main control, such as webpages. The TLRI considers that the right to correction in the PIPA should be similarly expanded to cover online publications over which personal information custodians maintain control, on the basis that this can provide important protection against the potential harms of misleading or inaccurate information online.[663]

6.6.26 The TLRI observes the Privacy Act Review's recommendation that individual rights in the Privacy Act should be accompanied by exceptions relating to the public interest, legal requirements and technical infeasibility and abuse of process (see [6.4.20] above). The TLRI considers that corresponding exceptions should accompany individual rights to access and explanation, erasure, and correction discussed in this sub-section, and to the right to object discussed at [5.4.40] and following, above.

6.6.27 The TLRI also considers that imposing requirements on personal information custodians to provide 'reasonable assistance' to individuals in exercising a right, take 'reasonable steps' to respond to an exercise of a right, and respond within a prescribed timeframe, unless a longer period is justified (also proposed by the Privacy Act Review), would be an appropriate way to balance individuals' rights with the administrative burden of compliance, although only with adequate resourcing for personal information custodians (discussed further at [6.6.18] and [6.6.19] above).

6.6.28 The TLRI notes that there are several other differences between PIPP 6 and APP 13 in relation to correction of personal information, but received no submissions on them and has subsequently not formed a view on their significance. They are:

- the additional ground for correction of 'irrelevant' found in APP 13;
- the additional obligation on APP entities to take reasonable steps, where practical and lawful, to notify third parties to whom personal information has previously been disclosed when the first entity has corrected that personal information.[664]

6.7 Recommendations

Recommendation 34: PIPP 4 should be amended, in line with the corresponding proposals of the Commonwealth Privacy Act Review, to:

- provide further guidance to personal information custodians on the 'reasonable steps' they must take to protect personal information;
- set baseline privacy outcomes personal information custodians must meet to fulfil their data security obligations; and
- require personal information custodians to set and periodically review retention periods for personal information.

[663] Privacy Act Review Report 2022 177.
[664] See [6.3.13] above.

Recommendation 35: Consideration should be given to whether further guidance on PIPA-compliant destruction and de-identification of personal information by personal information custodians, similar to the revised guidance proposed by the Commonwealth Privacy Act Review, is necessary.

Recommendation 36: An individual 'right to erasure', with the same features as the right proposed by the Commonwealth Privacy Act Review, should be introduced in the PIPA.

Recommendation 37: There should be a review of all Tasmanian legislation that requires retention of personal information to ensure it appropriately balances policy objectives with privacy and cyber-security risks.

Recommendation 38: PIPP 6 should be amended to require a personal information custodian to:

- provide individuals with access to their personal information upon request;
- provide access to personal information in the manner requested by the individual, as long as this is reasonable and practicable, without charge;
- give written notice of the reasons for a refusal to give access and the mechanisms available to complain about the refusal (which are discussed further in Part 8 of this Report); and
- adopt a presumption in favour of disclosure.

Recommendation 39: PIPP 6 should be amended to simplify the process for requesting access to personal information. These amendments should clarify the interaction of the PIPA and the RTI Act.

Recommendation 40: PIPP 6 should be amended to confer an individual right to explanation about personal information, including a right to explanation of the source of personal information collected indirectly, and a right to an explanation or summary of what a personal information custodian has done with the personal information.[665]

Recommendation 41: Part 3A of the PIPA should be amended to:

- modify the operation of Section 17G to enable a person to request (rather than require) the personal information custodian to add information to a notation;
- require a personal information custodian to provide a written notice of a refusal of a request to add information to a notation; and
- extend the right to correction in Section 17A to enable persons to request amendment of incorrect, incomplete, out-of-date, or misleading information in generally available publications online over which a personal information custodian maintains control.

Recommendation 42: Individual rights to access and explanation, to object, to erasure, and to correction in the PIPA should be subject to the exceptions proposed by the Commonwealth Privacy Act Review; namely, where:

- there are competing public interests;
- required or authorised by law or legal relationships; and
- technically infeasible or an abuse of process.

Recommendation 43: Personal information custodians should be required to provide 'reasonable assistance' to individuals in exercising a right, take 'reasonable steps' to respond to an exercise of a right, and respond within a prescribed timeframe, unless a longer period is justified.

[665] See Privacy Act Review Report 2022 Proposal 18.1.

Part 7

Aligning the Personal Information Protection Principles with the Commonwealth Act: Other Privacy Principles

7.1 Overview of this Part

7.1.1 This Part considers other issues that are dealt with in the Tasmanian Personal Information Protection Principles ('PIPPs')—requirements relating to openness (which require personal information custodians to prepare and publicise privacy policies), limitations on personal information custodians' use of unique identifiers, and obligations on custodians to give individuals the option of anonymity (PIPPs 5, 7 and 8)—and examines the adequacy of these principles *per se* and in comparison to the Australian Privacy Principles ('APPs').

7.1.2 This Part also discusses several matters raised in the Commonwealth Privacy Act Review which are not currently addressed in the Tasmanian privacy legislation but may have relevance for future reforms to the *Personal Information Protection Act 2004* (Tas) ('PIPA'). These concern use of personal information for targeting and direct marketing, and trading of information.

7.2 Openness and privacy policies

The Tasmanian position

7.2.1 Under Tasmanian law, PIPP 5 on 'openness' specifies that a personal information custodian must:

- 'clearly set out in a document its policies on its management of personal information';
- 'make the document available to anyone who asks for it'; and
- take reasonable steps to advise a person, on request, of the sort of information it holds, the purposes for which it holds the information, and how it collects, holds, uses, and discloses that information.

The position in other jurisdictions

7.2.2 Some other State and Territory jurisdictions, such as Victoria, the ACT, and the Northern Territory, articulate a similar privacy principle of openness, requiring regulated entities to clearly

express and make available their personal information management policies and to take reasonable steps to inform individuals about their practices upon request.[666]

7.2.3 The Commonwealth imposes similar but more expansive obligations relating to 'open and transparent management of personal information' in APP 1, which states that APP entities must have 'a clearly expressed and up-to-date policy … about the management of personal information'. It further holds that APP entities must take reasonable steps to make these policies publicly available free of charge and in an appropriate form, and in the form requested.[667]

7.2.4 Unlike PIPP 5, APP 1 specifies that privacy policies must contain certain information, including information on:

- the kinds of personal information the entity collects and holds;
- how the entity collects and holds the information;
- the purposes for which the entity collects, uses, and discloses personal information;
- how an individual may access their personal information and seek to have it corrected;
- how an individual may complain about a privacy breach; and
- if the entity is likely to disclose personal information to overseas recipients, the countries in which recipients are likely to be located (where practicable).[668]

7.2.5 Unlike PIPP 5, APP 1 also addresses wider governance and compliance mechanisms of APP entities. It requires APP entities to take reasonable steps to implement practices, procedures, and systems to ensure compliance with their privacy obligations and to enable the entity to deal with inquiries or complaints. To implement this requirement (found in APP 1.2), the Office of the Australian Information Commissioner ('OAIC') developed the Privacy (Australian Government Agencies – Governance) APP Code 2017 ('2017 APP Code').[669] This is registered under the *Privacy Act 1988* (Cth) ('Privacy Act') as an 'APP code'—a code of practice that sets out how one or more of the APPs are to be complied with, and which has the same legally binding effect as the APPs themselves.[670]

7.2.6 The 2017 APP Code establishes various measures that agencies must put in place in order to comply with APP 1.2, including obligations to:

- create a privacy management plan;
- designate privacy officers and privacy champions;
- provide appropriate privacy education and training for all new and continuing staff;
- conduct regular reviews of internal privacy processes; and
- conduct a privacy impact assessment for all privacy projects which are likely to have a significant impact on the privacy of individuals (that is, high risk privacy projects), and to make the assessment publicly available and listed on a publicly available register.

---

[666] *Privacy and Data Protection Act 2014* (Vic) sch 1, cl 5; IPA (ACT) TPP 1; *Information Act 2002* (NT) sch 2, cl 5.1, 5.2.
[667] *Privacy Act 1988* (Cth) APPs 1.3, 1.6.
[668] *Privacy Act 1988* (Cth) APP 1.4.
[669] OAIC*, Privacy (Australian Government – Agencies Governance) APP Code* (2017) <https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/australian-government-agencies-privacy-code/>.
[670] See *Privacy Act 1988* (Cth) Pt IIIB.

7.3 Proposals in the Commonwealth Privacy Act Review

7.3.1 The Privacy Act Review Final Report recommended a number of changes to the Privacy Act requirements relating to APP 1 privacy policies and compliance policies, procedures, and systems.

7.3.2 The Review recommended that APP entities' personal information retention periods be added to the list of information that APP entities are required to include in their privacy policies (which related to the proposal that APP entities be required to specify data retention periods.[671] The Government agreed in-principle with this proposal.[672]

7.3.3 The Review further proposed that standardised templates and layouts and related materials for collection notices and privacy policies should be developed through OAIC guidance or codes, on the basis that standardising communication with consumers could assist APP entities with compliance and consumers with comprehension of the content and meaning of notices and policies.[673] The Government agreed in-principle with this proposal.[674]

7.3.4 The Review also proposed that entities exempted from Privacy Act requirements under the political exemption (discussed in this Report at [5.4.5] and following) be required to publish a privacy policy, on the basis that this would enhance transparency about how political entities handle personal information and for what acts and practices.[675] The Government noted this proposal.[676]

7.3.5 The Review further proposed that the requirement for agencies to undertake privacy impact assessments in relation to 'high privacy risk projects' (currently dealt with in the 2017 APP Code) be inserted into the Privacy Act and extended to apply to all APP entities in relation to all activities with high privacy risks.[677] The Government agreed in-principle with this proposal.[678] The Review defined high privacy risk activities as activities that are 'likely to have a significant impact on the privacy of individuals'[679] and indicated that high privacy risk activities may include practices such as the collection, use, or disclosure of sensitive information or children's personal information on a large scale, ongoing or real-time tracking of individuals' geolocation, and sale of personal information.[680]

7.3.6 The Review further recommended that the Privacy Act be amended to require APP entities to appoint or designate a senior employee responsible for privacy. The report noted that this obligation already applies to public sector agencies by virtue of the 2017 APP Code, and that it is 'an important

[671] Privacy Act Review Report 2022 Proposal 21.8.
[672] Government Response 9.
[673] Privacy Act Review Report Proposal 10.3 and 99–100.
[674] Government Response 17.
[675] Privacy Act Review Report 2022 Proposal 8.2 and 75.
[676] Government Response 24.
[677] Privacy Act Review Report 2022 Proposal 13.1 and 124–125. The Review also recommended the development of OAIC guidance which articulated a non-exhaustive list of factors that indicate when an individual may be experiencing vulnerability and be at a higher risk of harm from interferences with their personal information: Proposal 17.1 and 159–162. The Government agreed with this proposal: Government Response 14.
[678] Government Response 10.
[679] Privacy Act Review Report Proposal 13.1. In this proposal, the Review also suggested that such a change be supported by OAIC guidance on the factors that might indicate a high privacy risk, and that an indicative list of high-risk practices could be included in the Act: ibid 124.
[680] Ibid.

feature of overseas privacy frameworks', such as the European Union's General Data Protection Regulation 2016/679 ('GDPR').[681] The Government agreed in-principle with this proposal.[682]

Automated decision-making

7.3.7 In the context of privacy policies and approaches to data management and privacy compliance, the Review also considered the potential privacy impacts of the proliferation of automated decision-making and artificial intelligence-enabled tools and their use by government and non-government entities.

7.3.8 The Review defined automated decision-making as the 'deployment of technology to automate a decision-making process', ranging from simple rules-based systems to the use of artificial intelligence ('AI').[683] The Review observed that submitters had noted both potential benefits and risks of the growing use of automated decision-making in the government and private sectors, including that they may promote efficiency, accuracy, and consistency of decisions, but may also entrench or produce bias leading to discrimination or unfair treatment.[684]

7.3.9 The Review discussed regulation of automated decisions under the GDPR. Article 22 of the GDPR provides various restrictions on the use of automated decision-making involving the use or generation of personal information, including profiling. Profiling involves using an automated process to analyse or predict a person's attributes or characteristics based on their personal information, often in combination with information collected from others.[685] Profiling can include using previous choices or behaviours, such as purchasing or browsing habits, to predict an individual's economic situation, health, preferences, interests, behaviour, or location.

7.3.10 Article 22 of the GDPR prevents a decision from being based *solely* on automated processing, if that decision has legal or similarly significant effects on the person. Even where automated processes can be used, further requirements exist depending on the type of information being used, as follows:

- *Sensitive* data: can only be used in automated processes where explicit consent has been given or it is authorised by legislation.
- *Non-sensitive* data: can only be used where necessary for various purposes, including: the performance of a contract with the individual; where it is authorised by legislation; or where the individual has explicitly consented to that use of their data.

7.3.11 In all cases, suitable measures must be taken to safeguard the interests of the individual concerned. This includes enabling the individual to request that a human be involved before any final decision or action is taken, to express their point of view, and to contest the decision.

7.3.12 The Australian Human Rights Commission ('AHRC') has recognised the difficulties associated with regulating the use of AI, including the technical complexity of developing and understanding the operation of AI systems. In light of this, the AHRC made recommendations relating

[681] Privacy Act Review Report 2022 Proposal 15.2 and 143–144. Legislation in most States and Territories does not require regulated entities to appoint a responsible privacy officer, although the Queensland legislation specifies that access and amendment requests to agencies must be dealt with by the agency's principal officer, who may delegate the power to another officer: *Information Privacy Act 2009* (Qld) s 50.
[682] Government Response 10.
[683] Privacy Act Review Report 2022 188.
[684] Ibid 188–189.
[685] See, eg, GDPR art 4 (definition of 'profiling').

to governments' use of AI-informed decision-making systems for administrative decision-making.[686] The recommendations included:

- carrying out a 'Human Rights Impact Assessment' before the system is used in order to evaluate its possible impacts on human rights, including how the system impacts privacy and whether it provides for appropriate review of decisions by human decision-makers;[687]
- providing for mechanisms to independently review the merits of any decision made;[688]
- requiring the use of AI to be specifically authorised and governed by legislation;
- requiring individuals to be notified before AI is used in a material way in decisions which may affect an individual's interests;
- informing individuals on how they can challenge a decision where AI has been used in a material way;[689] and
- requiring reasons or a technical explanation of the decision to be given before a decision can be considered lawful.[690]

7.3.13 In response, the Review proposed in its Final Report that:

- privacy policies should 'set out the types of personal information that will be used in substantially automated decisions which have a legal or similarly significant effect on an individual's rights';[691]
- the Privacy Act should be amended to include '[h]igh-level indicators of the types of decisions with a legal or similarly significant effect on an individual's rights', to be supplemented by OAIC guidance (which could be based on existing guidance produced overseas);[692] and
- a right of individuals to request meaningful information about how substantially automated decisions with legal or similarly significant effect are made should be introduced, as part of work underway by the Commonwealth Department of Industry, Science and Resources and wider work on the regulation of AI and automated decision-making ('ADM') (to ensure consistency and limit regulatory burden).[693]

7.4 Consultation

7.4.1 The TLRI Issues Paper did not pose any questions that explicitly dealt with privacy policies or openness more generally. It did pose one question about artificial intelligence:

> Should any of the other potential reforms be introduced, including:
>
> ...

[686] AHRC, *Human Rights and Technology Final Report* ch 5.
[687] Ibid 55 (Recommendation 2).
[688] Ibid 68 (Recommendation 8).
[689] Ibid 60 (Recommendation 3).
[690] Ibid 62 (Recommendation 5).
[691] Privacy Act Review Report 2022 Proposal 19.1.
[692] Ibid Proposal 19.2 and 190.
[693] Ibid Proposal 19.3 and 193. The Review explained that the use of 'substantially automated decisions' rather than the GDPR language of 'solely automated decisions' was intended to ensure that entities could not avoid their obligations by introducing negligible human involvement in decision-making, and was consistent with the way the GDPR requirement had been interpreted: ibid 193.

specific restrictions on the use of artificial intelligence in automated administrative decision-making[694]

7.4.2 Meg Webb MLC expressed a concern about automated decision-making; Ms Webb and several other submitters raised the issue of the potential for profiling in relation to private sector use of facial recognition technology ('FRT').[695] For example, the Tasmanian Council of Social Service ('TasCOSS') cited the AHRC's *Human Rights and Technology* Final Report in support of its submission that FRT raises a range of concerns, including with the use of data in police profiling and the disproportionate impact of errors with FRT and its use on 'certain groups'[696] (see further [4.9.3] of this Report).

7.4.3 Also relevant to the design of privacy policies was Ms Webb's submission ([5.6.6] above in relation to collection notices) that individuals should be informed of the intended duration of data storage, expected timeframe for deletion or partial deletion (if appropriate), and when erasure has occurred.[697]

7.5 The TLRI's view

7.5.1 The TLRI observes that the PIPA provisions relating to openness and privacy policies are very similar to those found in other State and Territory legislation. These provisions are, however, inconsistent with the Commonwealth Privacy Act, which contains a greater level of detail and prescribes additional requirements (either directly or via the APP Code 2017) relating to regulated entities' protection of information and compliance with the legislation.[698]

7.5.2 The TLRI considers that there may be advantages, in terms of providing clarity and guidance for personal information custodians and equipping individuals with more information about their privacy, to:

- amending the PIPA to align more closely with the Privacy Act by specifying the types of information that must be included in privacy policies (similar to the list in APP 1.4, which the Privacy Act Review recommended should be amended to include information about retention periods); and
- legislating the requirement for all personal information custodians to designate a privacy officer (similar to the requirement in 2017 APP Code, which the Privacy Act Review recommended be imported into the Privacy Act itself). It is acknowledged that Tasmanian agencies may already have privacy officers, although it is notable that the Commission of Inquiry into the Tasmanian Government's Responses to Child Sexual Abuse in Institutional Settings ('CoI') commented on a lack of designated staff appointed to deal with PIPA requests.[699]

7.5.3 As with other recommendations made in this Report, the implementation of these recommendations would require consideration of whether personal information custodians have adequate resources and support to implement them.

[694] Issues Paper Part 2, Question 2.9(d).
[695] Submission 8 (Meg Webb MLC).
[696] Submission 11 (TasCOSS) 5.
[697] Submission 8 (Meg Webb MLC).
[698] It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.
[699] CoI Report 190–191; see Part 6 above.

7.5.4 The TLRI notes the concerns raised by multiple submitters about the privacy risks associated with emerging technology, such as FRT and ADM. The TLRI agrees with the findings of the Commonwealth Privacy Act Review and other recent projects (such as the AHRC's *Human Rights and Technology* project) that the risks associated with these technologies justify reforms to privacy legislation.

7.5.5 The TLRI considers that the PIPA should be strengthened by:

- requiring personal information custodians to specify types of personal information that will be used in ADM (with appropriate guidance for personal information custodians); and
- establishing a right to request meaningful information about how such decisions are made.

7.5.6 The TLRI notes that the recommendations of the Privacy Act Review in this regard are similar to regulations in other data protection regulatory schemes, such as the GDPR.[700]

7.6 Recommendations

Recommendation 44: There should be greater clarity around how personal information custodians should meet the requirements of PIPP 5. This should include:

- specifying the type of information that must be included in privacy policies made under PIPP5; and
- requiring personal information custodians to designate a senior employee as privacy officer responsible for compliance with the PIPA.

This could be implemented by amendment to legislation or regulation, or the development of guidelines.

Recommendation 45: The PIPA should be amended to:

- require personal information custodians to specify the types of personal information that will be used in automated decision-making; and
- establish a right to request meaningful information about how such decisions are made.

Recommendation 46: Guidance should be developed to support personal information custodians to meet new requirements relating to automated decision-making.

7.7 Unique identifiers

The Tasmanian position

7.7.1 The PIPA defines an 'identifier' as 'anything assigned by a personal information custodian to an individual to identify them for its operations, other than a name or ABN [Australian Business Number]'.[701]

[700] Privacy Act Review Report 2022 189.
[701] PIPA s 3 (definition of 'identifier').

7.7.2 PIPP 7 restricts the use of unique identifiers. It prohibits a personal information custodian from assigning a unique identifier to an individual, unless it is necessary to carry out any of the custodian's functions efficiently.[702]

7.7.3 Further, a personal information custodian cannot adopt a unique identifier that was assigned by another personal information custodian, unless:

- the adoption is necessary to carry out the personal information custodian's functions;
- the individual has consented; or
- the personal information custodian is 'a body, organisation or individual adopting the identifier created by a personal information custodian in the performance of its obligations to the personal information custodian under a personal information contract'.[703]

7.7.4 PIPP 7 also specifies that a personal information custodian must not use or disclose a unique identifier assigned by another personal information custodian, unless it is necessary to fulfil its obligations to the other personal information custodian or PIPP 2(1) relating to permitted use and disclosure of personal information applies (see Part 5 of this Report).

The position in other jurisdictions

7.7.5 The Privacy Act defines an 'identifier' as a number, letter, or symbol, or combination of these, that is used to identify an individual or verify their identity.[704] The privacy legislation in other jurisdictions also contains a definition of 'identifier' or 'unique identifier' as, variously, 'an identifier … which is usually but need not be a number',[705] 'usually a number',[706] or a code.[707] A 'government related identifier' is defined as one that has been assigned by an agency, a State or Territory authority, an agent of either such body, or a contracted service provider for a Commonwealth contract or State contract, where acting in its capacity as a contracted service provider.[708]

7.7.6 The relevant principles that apply to unique identifiers in Victoria and the Northern Territory are similar to the PIPA.[709] In contrast, unlike the PIPA, the Privacy Act only addresses the adoption, use, or disclosure of government related identifiers. The relevant privacy principle (APP 9) restricts the use of such identifiers by *non-government* organisations.[710]

7.7.7 APP 9 holds that an organisation cannot adopt a government related identifier, unless authorised by law, and cannot use or disclose a government related identified, unless it is:

---

[702] For a discussion of how to identify a custodian's functions, see the discussion in relation to PIPP 1, above at [5.2.1].
[703] PIPP 7(2).
[704] *Privacy Act 1988* (Cth) s 6(1).
[705] PPIP Act (NSW) s 59R.
[706] PDP Act (Vic) IPP 7.
[707] *Information Act* (NT) s 4. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) sets out the definition of identifier by the new chapter 3 inserted by s 33 (yet to commence).
[708] *Privacy Act 1988* (Cth) s 6(1). OAIC guidance notes that other laws regulate the collection, use or disclosure of particular identifiers such as tax file numbers: OAIC, *APP Guidelines* [9.9].
[709] PDP Act (Vic) IPP 7; *Information Act* (NT) IPP 7.
[710] It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP but there is no QPP the equivalent of APP 9.

- reasonably necessary to verify the individual's identity for the purposes of the organisation's activities or functions;
- reasonably necessary for the organisation to fulfil its obligations to an agency or a State or Territory authority;
- required or authorised under an Australian law or court or tribunal order;
- a situation that constitutes a 'permitted general situation' where information or identifiers can be used or disclosed;[711] or
- it is reasonably believed by the organisation to be necessary for one or more enforcement related activities conducted by or on behalf of an enforcement body.[712]

7.7.8 In contrast to the restriction on the adoption, use, and disclosure of government related identified by organisations, the adoption, use, and disclosure of identifiers by (government) agencies is not generally restricted, except insofar as it is subject to the APPs where an identifier amounts to personal information.[713]

7.8 Proposals in the Commonwealth Privacy Act Review

7.8.1 The Privacy Act Review Final Report did not make any recommendations in relation to APP9 or unique identifiers more generally.

7.9 Consultation

7.9.1 The TLRI Issues Paper did not pose any questions about PIPP 7 or unique identifiers. The TLRI did not receive any submissions that addressed this matter.

7.10 The TLRI's view

7.10.1 The TLRI observes that the PIPA is more restrictive than the Privacy Act in its treatment of identifiers assigned by government or other public bodies. In light of the fact that no submitters raised concerns about this, and that PIPP 7 permits custodians to adopt identifiers where necessary to carry out the custodian's functions, where the individual has consented, or where it is in the performance of obligations under a personal information contract, the TLRI is of the view that no reforms to PIPP 7 are necessary.

---

[711] For example, where it is unreasonable or impracticable to obtain consent of the individual, and the use or disclosure is necessary to prevent a serious threat to life, health, or safety: *Privacy Act 1988* (Cth) s 16A.

[712] APP 9.2.

[713] The OAIC guidelines specify that identifiers will constitute personal information 'if the individual is identifiable or reasonably identifiable from the identifier, including from other information held by, or available to, the entity that holds the identifier': OAIC, *APP Guidelines* [9.4]. One exception to this, established in s 7A of the Privacy Act, specifies that the acts of agencies will be treated as acts of organisations (and hence be subject to APP 9) where the agency is listed in Part I of Schedule 2 of the *Freedom of Information Act 1982* ('FOI Act') and is prescribed in regulations, or where the act or practice relates to the commercial activity of the agency or another entity and the agency is specified in Part II of Schedule 2 of the FOI Act: *Privacy Act 1988* (Cth) s 7A; see OAIC, *APP Guidelines* [9.11].

7.11 Recommendations

7.11.1 The TLRI makes no recommendations in relation to PIPP 7.

7.12 Anonymity

The Tasmanian position

7.12.1 PIPP 8 addresses anonymity and states that, '[w]herever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with a personal information custodian'.

The position in other jurisdictions

7.12.2 Legislation in some other States and Territories, including Victoria, the ACT, and the Northern Territory, contains a near-identical provision to PIPP 8.[714]

7.12.3 Under the Commonwealth Privacy Act, APP 2 (titled 'anonymity and pseudonymity') states that, '[i]ndividuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity'.[715] It holds that this does not apply where the entity is authorised or required by law to deal with individuals who have identified themselves, or where it is impracticable for the entity to deal with individuals who have not identified themselves or who have used a pseudonym.

7.13 The Commonwealth Privacy Act Review

7.13.1 The Privacy Act Review Final Report did not make any recommendations in relation to the option of anonymity or APP 2.

7.14 Consultation

7.14.1 The TLRI Issues Paper did not pose any questions about anonymity. The TLRI did not receive any submissions that addressed this matter.

7.15 The TLRI's view

7.15.1 The TLRI observes that the inclusion in the Privacy Act's APP 2 of optional use of a pseudonym may extend the range of lawful and practicable options available to individuals seeking to avoid identification beyond the option compared to the more general 'option of not identifying

[714] *Privacy and Data Protection Act 2014* (Vic) sch 2, cl 8; *Information Act 2002* (NT) sch 2, cl 8.1; *Information Privacy Act 2014* (ACT) TPP 2. See also *Information Privacy Act 2009* (Qld) sch 4, cl 8 which applies to health agencies.

[715] It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) replaces IPP with QPP set out in schedule 3 (yet to commence). The new schedule 3 is based on the APP.

themselves' which must be offered under the PIPA and equivalent provisions in other State and Territory legislation. However, as discussed above at [4.2.12] regarding de-identification, pseudonymous information may no longer be considered 'personal information' and hence will not attract privacy protections, since the identity of an individual is no longer apparent or reasonably ascertainable.

7.15.2 The TLRI has not formed a view regarding whether the PIPA should be amended to align it with the Commonwealth Privacy Act by introducing the option for individuals to use a pseudonym where they do not want to be identified.

7.16 Recommendations

7.16.1 The TLRI makes no recommendations in relation to PIPP 8.

7.17 Other PIPA-related issues requiring further consideration

7.17.1 Several other matters mentioned in the Privacy Act Review's Final Report may have a bearing on any future reforms of Tasmania's PIPA and will need to be considered once the shape of reforms to the Privacy Act is finalised. These include:

- proposals relating to targeting (where information is collected, used, or disclosed to tailor services, content, information, advertisements, or offers),[716] such as proposals to give individuals a right to opt-out of receiving targeted advertising,[717] to prohibit targeting to children except where in a child's best interests,[718] to prohibit targeting of individuals based on sensitive information,[719] to require entities to provide information about targeting,[720] and to make regulation of tailored content apply to de-identified information;[721] and
- proposals relating to trading (where information is disclosed for a benefit, service, or advantage),[722] including proposals to restrict trading of personal information without an individual's consent,[723] and to prohibit trading in the personal information of children.[724]

7.17.2 The Privacy Act Review also made several proposals relating to direct marketing (where information is handled for the purpose of communicating directly with an individual to promote advertising or marketing material).[725] These included proposals to give individuals a right to opt-out[726] and to prohibit direct marketing to children except in limited circumstances (such as where it is in the

[716] Privacy Act Review Report 2022 Proposal 20.1.
[717] Ibid Proposal 20.3. The Government noted this proposal: Government Response 13.
[718] Ibid Proposal 20.6. The Government agreed in-principle with this proposal: Government Response 13.
[719] Ibid Proposal 20.8. The Government agreed in-principle with this proposal: Government Response 12.
[720] Ibid Proposal 20.9. The Government agreed in-principle with this proposal: Government Response 12.
[721] Ibid Proposal 4.6(a).
[722] Ibid Proposal 20.1. The Government agreed in-principle with this proposal: Government Response 12.
[723] Ibid Proposal 20.4. The Government agreed in-principle with this proposal: Government Response 12.
[724] Privacy Act Review Report 2022 Proposal 20.7.
[725] Ibid Proposal 20.1.
[726] Ibid Proposal 20.2.

best interests of the child).[727] The Commonwealth Government agreed in-principle with these proposals.[728]

7.17.3 The TLRI also observes that the PIPA does not impose specific obligations regarding use and disclosure of personal information for direct marketing. This means that, while non-government contractors and their sub-contractors must comply with the PIPPs, they are not subject to additional restrictions regarding the use or disclosure of personal information for direct marketing purposes. If the direct marketing purpose is relevant to the primary purpose for collecting the information, the information does not have to be collected from the marketing subject, nor does the subject need to consent to the use of their information for direct marketing purposes. While the TLRI did not receive submissions on this point, it considers that further consideration of this gap in the legislation, in light of the Privacy Act Review Report proposals, may be warranted.

[727] Privacy Act Review Report 2022 Proposal 20.5.
[728] Government Response 12–13.

Part 8

The PIPA: Complaints, Monitoring, and Enforcement

8.1 Introduction

8.1.1 Complaints, monitoring, and enforcement mechanisms are essential elements of effective information privacy protections. This Part considers the adequacy of the complaints and appeals processes in the *Personal Information Protection Act 2004 (Tas)* ('PIPA'), remedies, and other enforcement action available in response to breaches (including data breach notification requirements), and the need for privacy codes or other rules in delegated legislation to be developed.

8.2 Complaints and remedies

The Tasmanian position

The complaints process

8.2.1 Under the Tasmanian PIPA, a person may make a complaint to the Tasmanian Ombudsman alleging that a personal information custodian has contravened a Personal Information Protection Principle ('PIPP') which applies to the person.[729] Complaints must be made within six months from the date the person first became aware of the alleged breach, unless the Ombudsman permits additional time.[730]

8.2.2 Before a complainant can make a complaint to the Ombudsman, however, they must have raised the matter with the relevant personal information custodian and be unsatisfied with the response.[731]

8.2.3 If these requirements are met, the Ombudsman may conduct a preliminary assessment of the complaint for the purpose of deciding whether to deal with the complaint.[732] If, following a preliminary assessment, the Ombudsman believes the complaint may be resolved expeditiously (having regard to the nature and seriousness of the complaint), the Ombudsman may resolve the complaint without investigating it further.[733]

8.2.4 Alternatively, the Ombudsman may decide not to deal with a complaint, if satisfied that:

- the complaint is frivolous, vexatious, lacking in substance, or not in good faith;

[729] PIPA s 18(1), (2).
[730] If the complaint is about the custodian refusing a request to amend personal information, the complainant only has 20 working days of them being notified of the refusal: ibid s 18(5).
[731] PIPA s 18(1).
[732] PIPA s 19.
[733] PIPA s 19(1A).

- the subject matter of the complaint is trivial; or
- the subject matter of the complaint relates to a matter permitted or required under any law.[734]

8.2.5 The Ombudsman may also refer a complaint for investigation or other action to any person, body, or authority the Ombudsman considers appropriate; such referral must only take place after consultation of, and consideration of the views of, both the complainant and relevant person, body, or authority.[735]

8.2.6 If the Ombudsman decides to deal with a complaint, the PIPA requires the Ombudsman to conduct any investigations in accordance with the process and powers set out in Division 3 of Part III of the *Ombudsman Act 1978* (Tas).[736] That Act provides, for example, that:

- the Ombudsman must give written notice of the intention to investigate to the complainant and the public authority;[737]
- the Ombudsman may regulate investigation procedure, obtain information, and make any inquiries in a manner they consider appropriate, and is not required to hold a hearing;[738]
- an investigation by the Ombudsman must be conducted in private;[739]
- the Ombudsman must not make a report on an investigation containing adverse or derogatory comments in respect of a person, or a public authority, without giving the person, or the principal officer and principal decision-maker, the opportunity to appear before the Ombudsman or otherwise make representations[740]
- the Ombudsman has extensive powers, including compelling people to provide information or give evidence,[741] and entering the premises of public authorities.[742]

8.2.7 If the Ombudsman determines, upon completion of an investigation, that the custodian has breached a PIPP, the Ombudsman must advise the complainant and custodian of the reasons for that opinion and may make any recommendations the Ombudsman considers appropriate.[743] The Ombudsman must provide the opinion and any recommendations to the Minister; these must be tabled in both Houses of Parliament within five sitting days of receipt.[744]

8.2.8 Table 8.1, below, sets out the number of privacy complaints received by agency type, according to the Ombudsman's recent annual reports.[745]

[734] PIPA s 19(2).
[735] PIPA s 20.
[736] PIPA s 21.
[737] *Ombudsman Act 1978* (Tas) 23(1).
[738] *Ombudsman Act 1978* (Tas) 23A(1)
[739] *Ombudsman Act 1978* (Tas) s 23A(3).
[740] *Ombudsman Act 1978* (Tas) s 23A(5), (6).
[741] *Ombudsman Act 1978* (Tas) s 24.
[742] *Ombudsman Act 1978* (Tas) s 25.
[743] PIPA s 22(1).
[744] PIPA s 22(2) and (3).
[745] Ombudsman Tasmania, *Annual Report 2021–2022* (Report, 2022) 12 <https://www.ombudsman.tas.gov.au/__data/assets/pdf_file/0007/683251/Final-signed-Ombudsman-Annual-Report-2021-2022.PDF>.

Table 8.1 Number of privacy complaints to Tasmanian Ombudsman 2018–23 by agency type (%)

Agency	2018–19 N (%)	2019–20 N (%)	2020–21 N (%)	2021–22 N (%)	2022–23 N (%)
State government departments	382 (52.5)	344 (53.5)	378 (53)	508 (56)	415 (55)
Local government	76 (10.5)	81 (12.7)	77 (13)	88 (10)	74 (10)
Public authorities and GBEs	119 (16.2)	66 (10.3)	69 (10)	93 (10)	71 (9)
Out of jurisdiction	150 (20.6)	131 (20.4)	170 (20)	188 (21)	167 (22)
Personal Information Protection	4 (<1)	14 (2.1)	17 (3)	11 (1)	19 (3)
Public Interest Disclosure	4 (<1)	6 (1)	4 (1)	19 (2)	10 (1)
Total	**735 (100)**	**642 (100)**	**715 (100)**	**907 (100)**	**756 (100)**

The appeals process

8.2.9 The PIPA does not make provision for an individual to seek merits review at the Tasmanian Civil and Administrative Tribunal ('TasCAT'), if they are dissatisfied with the actions or recommendations of the Ombudsman in response to a PIPA complaint. Judicial review of findings made by the Ombudsman in relation to PIPA will be available in the Supreme Court of Tasmania.[746]

Own-motion investigations

8.2.10 The Ombudsman can initiate an own motion investigation into administrative action taken by public authorities and government contractors, including information handling practices, under the *Ombudsman Act 1978* (Tas).[747] This appears to include powers of the Ombudsman to initiate own-motion investigations under the PIPA, although this is not made clear in the PIPA itself.[748]

Remedies for breach of privacy

8.2.11 The PIPA does not empower the Ombudsman to make orders for compensation for a breach of the PIPPs, nor does the PIPA provide for any penalties when a PIPP is breached.

[746] Noting that, under s 33(3) of the *Ombudsman Act 1978* (Tas), an injunction is not to be issued, and an order of review is not to be made under the *Judicial Review Act 2000* (Tas), if these would restrain the Ombudsman from carrying out, or compelling the Ombudsman to carry out, any investigation under this or any other Act.
[747] See *Ombudsman Act 1978* (Tas) s 12.
[748] See PIPA s 21, which provides for the Ombudsman to conduct an investigation into any general issue or matter under this Act; however, there is no indication that this provision, entitled 'Dealing with complaints', is intended to authorise investigations in the absence of a complaint. Cf *Privacy Act 1988* (Cth) s 40(2).

The position in other jurisdictions

The complaints process

8.2.12 Like the PIPA, information privacy legislation in other Australian States and Territories establishes complaint mechanisms for breaches. In some jurisdictions, the legislation establishes a privacy-specific office-holder, such as the New South Wales Privacy Commissioner ('NSWPC'), who is responsible for dealing with complaints, among a range of other functions.[749] In other jurisdictions, such as Victoria and Queensland, one office-holder—the Victorian Information Commissioner ('VIC') and the Queensland Information Commissioner ('QIC'), respectively—is responsible for privacy and other areas of law relating to information and/or public administration, such as freedom of information.[750]

8.2.13 The legislation in other jurisdictions provides ways for an individual to initiate a review of a potential breach which are broadly like those available under Tasmania's PIPA;[751] for example

- At the Commonwealth level, the Information Commissioner ('the Commissioner') is responsible for handling individuals' complaints about interferences with their privacy.[752] The Commissioner must investigate complaints about acts or practices that 'may be an interference' with privacy, but generally only if the complainant has first complained to the respondent directly.[753] The Commissioner must make a reasonable attempt to conciliate a complaint where they consider it reasonably possible the conciliation may be successful.[754] After an investigation, the Commissioner may either dismiss the complaint or determine that the complaint is substantiated and make a declaration (discussed below at [8.2.23]).[755]
- In Victoria, complainants can make a complaint to the VIC if they have previously made a complaint to the organisation the subject of the complaint.[756] If the VIC decides to entertain the complaint and considers it reasonably possible the complaint may be conciliated successfully, it must attempt to resolve it through conciliation.[757] If conciliation is successful, the outcome may, at the request of any party, be formalised in a written agreement.[758]
- In NSW, complaints may be made to (or by) the NSWPC about alleged violations of, or interference with, an individual's privacy.[759] Complaints about certain conduct, including contraventions of an information protection principle, may alternatively be subject to 'internal review' by the public sector agency.[760] The NSWPC may decline to investigate a complaint about such conduct, if it would be more appropriate for the complainant to make the application

[749] *Privacy and Personal Information Protection Act 1998* (NSW) ss 34, 36.
[750] *Freedom of Information Act 1982* (Vic) Part 2A; *Privacy and Data Protection Act 2014* (Vic) s 3; *Information Privacy Act 2009* (Qld) Ch 4 Pt 3.
[751] It is noted that legislation in other jurisdictions address similar details to PIPA such as power to refer complaints received to other bodies, time frames for responding to complaints and the like.
[752] *Privacy Act 1988* (Cth) s 36.
[753] *Privacy Act 1988* (Cth) s 40.
[754] *Privacy Act 1988* (Cth) 40A. The Commissioner must notify the complainant and respondent if the Commissioner is satisfied there is no reasonable likelihood the complaint will be resolved by conciliation, and may decide not to (further) investigate: ibid ss 40A(3), (4).
[755] *Privacy Act 1988* (Cth) 52(1).
[756] *Privacy and Data Protection Act 2014* (Vic) ss 57, 62(1)(c).
[757] *Privacy and Data Protection Act 2014* (Vic) s 67; see also VCAT, *Information Privacy Complaints* (Web Page) <https://www.vcat.vic.gov.au/case-types/privacy-and-health-records/information-privacy-complaints#:~:text=If%20you%20believe%20someone%20has,resolve%20your%20complaint%20through%20conciliation>.
[758] *Privacy and Data Protection Act 2014* (Vic) s 69.
[759] *Privacy and Personal Information Protection Act 1998* (NSW) s 45.
[760] *Privacy and Personal Information Protection Act 1998* (NSW) Pt 5.

directly to the agency.[761] Following a request for internal review, the NSWPC must be informed of the review and may make submissions or carry out the review at the request of the agency.[762] The NSWPC is required to 'endeavour to resolve' complaints via conciliation.[763]

- In Queensland, individuals may make privacy complaints about a relevant entity to the QIC after they have first complained to an appropriate person within the entity.[764] The QIC must take all reasonable steps to cause a complaint to be mediated if they consider mediation could resolve the complaint.[765] Certain decisions made under the Queensland legislation are 'reviewable decisions', including a decision that an access or amendment application is outside the scope of the Act, a decision that an access or amendment application does not comply with application requirements, and a decision to refuse to deal with an access or amendment application, among others.[766] A person affected by a reviewable decision can apply to:
    - have the decision reviewed by the agency or Minister dealing with the application (known as 'internal review'), after which the reviewer must make a new decision;[767] or
    - have the decision reviewed by the QIC,[768] following which (unless the QIC declines to review the decision),[769] the QIC must seek early resolution via mediation or settlement,[770] or, if this does not occur, must make a written decisions either affirming, varying, or setting aside and making a decision in substitution.[771]

The appeals process

8.2.14 Privacy legislation in other jurisdictions creates avenues for appealing initial decisions about privacy complaints.

8.2.15 At the Commonwealth level, individuals can seek to have decisions of the Commissioner reviewed by the Administrative Appeals Tribunal ('AAT')[772] or federal courts.[773] The AAT conducts

[761] *Privacy and Personal Information Protection Act 1998* (NSW) s 46(3)(e). If a complaint about a government agency is made directly to the Privacy Commissioner, the Commissioner must inform the complainant of the internal review process available and the remedial action that may be available if they complain directly to the agency: ibid s 46(2).
[762] *Privacy and Personal Information Protection Act 1998* (NSW) s 54. Complaints about private bodies can be made directly to the Privacy Commissioner, and where the Commissioner decides to deal with a complaint, it must endeavour to resolve the matter via conciliation: ibid s 49. The Commissioner may make a report as to any findings or recommendations in relation to the complaint: ibid s 50(1).
[763] *Privacy and Personal Information Protection Act 1998* (NSW) s 49.
[764] *Information Privacy Act 2009* (Qld) ss 165(1), (3)(a), 168. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) amends the provisions in relation to the complaint process (not yet commenced). It is noted that the reforms enhance the powers and functions of the Information Commissioner and enhance arrangements for privacy complaints: see Explanatory Memorandum 2, 4.
[765] *Information Privacy Act 2009* (Qld) s 171.
[766] *Information Privacy Act 2009* (Qld) sch 5 (definition of 'reviewable decision'). It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) omits the definition of reviewable decision in Schedule 5.
[767] *Information Privacy Act 2009* (Qld) ss 93–97. It is noted that Chapter 3 (ss 40–133) is replaced by a new Chapter 3 in the *Information Privacy and Other Legislation Amendment Act 2023* (Qld), which includes new provisions about internal and external review, and appeals to the QCAT (not yet commenced). This chapter also contains new provisions about mandatory data breach notifications.
[768] *Information Privacy Act 2009* (Qld) s 99.
[769] *Information Privacy Act 2009* (Qld) s 107.
[770] *Information Privacy Act 2009* (Qld) s 103.
[771] *Information Privacy Act 2009* (Qld) s 123.
[772] *Privacy Act 1988* (Cth) s 96.
[773] *Administrative Decisions (Judicial Review) Act 1977* (Cth) s 5; OAIC, *Guide to Privacy Regulatory Action* ch 4 [4.24].

merits review—reviewing both the factual and legal basis for the Commissioner's decision, and can set aside, vary, or affirm the decision. The courts conduct judicial review—meaning they only determine whether or not the decision was *lawful* (for example, whether the Commissioner properly exercised its powers under the law in arriving at the decision), not whether the decision held merit. If the review shows that the decision was *not* lawful, the court may refer the decision back to the Information Commissioner for re-consideration and decision, but cannot re-make the decision itself.

8.2.16 In Victoria, a complainant may require the VIC to refer their complaint to the Victorian Civil and Administrative Tribunal ('VCAT') for merits, review where conciliation is not appropriate or has failed.[774] The Minister can also directly refer complaints to the Tribunal.[775]

8.2.17 In New South Wales, decisions from an internal review of a complaint about an agency can be reviewed by the NSW Civil and Administrative Tribunal ('NCAT').[776]

8.2.18 In Queensland, there is a referral pathway for privacy complaints from the information commissioner to the Queensland Civil and Administrative Tribunal ('QCAT').[777]

8.2.19 The scope of remedies and outcomes available to these bodies is discussed at [8.2.22] and following, below.

Own-motion investigations

8.2.20 Authorities in other jurisdictions also have some powers to initiate investigations, regardless of whether a complaint has been made. For example, under the Commonwealth Privacy Act, the Commissioner may conduct an investigation on its own initiative, if the act or practice being investigated may constitute an interference with an individual's privacy or of APP 1 and the Commissioner thinks an investigation desirable.[778] After such an investigation, the Commissioner may make a determination similar to the determinations that may arise from the investigation of a complaint (see [8.2.23], below).[779]

8.2.21 The NSWPC may 'conduct such inquiries, and make such investigations, into privacy related matters as the Privacy Commissioner thinks appropriate'.[780] The Act clarifies that, where the Privacy Commissioner has declined to deal with, or has referred, a complaint, the Commissioner may still conduct an inquiry or investigation into general issues or matters raised in connection with the complaint.[781] The QIC also has powers to conduct reviews into information handling practices of relevant agencies.[782] Similarly, in Victoria, the VIC has the powers to examine the practice of an

[774] *Privacy and Data Protection Act 2014* (Vic) ss 66, 71.
[775] *Privacy and Data Protection Act 2014* (Vic) s 65.
[776] *Privacy and Personal Information Protection Act 1998* (NSW) ss 53(6), 55.
[777] See *Information Privacy Act 2009* (Qld) ss 174–178. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) amends the provisions in relation to the complaint process (not yet commenced). It is noted that the reforms enhance arrangements for privacy complaints: see Explanatory Memorandum 4.
[778] *Privacy Act 1988* (Cth) 40(2).
[779] *Privacy Act 1988* (Cth) 52(1A).
[780] *Privacy and Personal Information Protection Act 1998* (NSW) s 36(2)(l).
[781] *Privacy and Personal Information Protection Act 1998* (NSW) s 51.
[782] *Information Privacy Act 2009* (Qld) s 135. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) amends the provisions in relation to the complaint process (not yet commenced). It is noted that the reforms enhance the powers and functions of the Information Commissioner: see Explanatory Memorandum 2.

organisation with respect to personal information (amongst other powers).[783] In addition, in Victoria, the VIC can conduct investigations for the purpose of issuing a compliance notice for a serious, flagrant, or repeated breach of a Victorian privacy principle, code of practice (described at [8.2.32] below), or approved information usage arrangement.[784]

Remedies for breaches of privacy

8.2.22 The absence of a compensation mechanism and other remedies for breaches of the PIPA stands in contrast to the availability of a range of remedies under privacy legislation in other Australian jurisdictions.

8.2.23 At the Commonwealth level, after an investigation under the Privacy Act, the Commissioner can make a range of declarations,[785] including a declaration of one or more of the following:

- that there has been interference with the privacy of an individual and that the respondent must not repeat or continue such conduct;
- that the respondent must take specified steps within a specified period to ensure the conduct is not repeated or continue;
- that the respondent must perform any reasonable act or course of conduct to redress loss or damage (including humiliation or injury to feelings);
- that the respondent must prepare and publish, or otherwise communicate, a statement about the conduct;
- that the complainant is entitled to 'a specified amount by way of compensation' for loss or damage suffered (including for humiliation and injury to feelings);[786] and
- that any further action would be inappropriate.[787]

8.2.24 If compensation is ordered, the payable amount is enforceable as a debt due.[788]

8.2.25 In the period 2020–21, the Office of the Australian Information Commissioner ('OAIC') reported 71 conciliated privacy complaints in which compensation was an agreed remedy, with 11 complaints involving compensation of over $10,000.[789] Conciliated privacy complaints are where the OAIC assists parties to resolve the complaint between themselves, rather than determining it for them.

8.2.26 The Privacy Act also provides for a range of civil penalty measures associated with certain breaches under the Act; namely, in relation to a serious or repeated interference with privacy, or in relation to contravention of certain provisions relating to credit reporting.[790] These civil penalty provisions are enforceable via the Commissioner seeking a court order that the contravener pay a pecuniary penalty.[791] The OAIC has stated that, even if a civil penalty order is available, it will not decide in every case that such an order is the appropriate enforcement option.[792] According to the Final

[783] *Privacy and Data Protection Act 2014* (Vic) s 8C(2).
[784] *Privacy and Data Protection Act 2014* (Vic) s 78.
[785] *Privacy Act 1988* (Cth) s 52(1)(b)(iii).
[786] *Privacy Act 1988* (Cth) s 52(1AB).
[787] *Privacy Act 1988* (Cth) s 52(1).
[788] *Privacy Act 1988* (Cth) s 60.
[789] OAIC, *Annual Report 2020–21* (Report, September 2021) 127. The most recent annual report (2021-22) does not provide this information.
[790] *Privacy Act 1988* (Cth) s 13G.
[791] See *Privacy Act 1988* (Cth) s 80U.
[792] OAIC, *Guide to Privacy Regulatory Action* (Guidance Document, January 2023) ch 7 [7.22].

Report of the Privacy Act Review, the Commissioner has previously commenced one civil penalty proceeding for serious or repeated interferences with privacy.[793]

8.2.27 The Commissioner can also enforce provisions of the Privacy Act by seeking an injunction before, during, or after an investigation or exercise of other regulatory powers,[794] or by accepting an enforceable undertaking.[795] Enforceable undertakings are used where there has already been, or appears to have been, a privacy interference. An enforceable undertaking seeks to have the entity voluntarily agree to modify its acts, remedy any damage the breach caused, and commit to future measures to comply with privacy obligations.[796] The terms of an enforceable undertaking are negotiated between the entity and the OAIC and, if accepted by the Commissioner, are ultimately enforceable in court.[797]

8.2.28 The Privacy Act also permits individuals to seek an injunction in court to restrain an entity from contravening any provision in the Act or to require the entity to do a certain thing.[798] Other than these injunctions, there is no direct right of action to seek compensation or other orders from the court under the Privacy Act.

8.2.29 At the State and Territory level, tribunals (but not Privacy Commissioners or the equivalent) are empowered to making enforceable declarations in response to an appeal about a privacy complaint; for example

- In NSW, NCAT is empowered to make various orders against the public sector agency, including orders to stop or refrain from conduct, to perform a privacy principle, to apologise to the complainant, or to take steps to remedy any loss or damage.[799] NCAT may award damages not exceeding $40,000 as compensation for loss or damage.[800] Such decisions are enforceable.
- In Victoria, if VCAT finds part or all of a complaint proven, it may make a range of orders, including orders requiring the organisation to change its practices, to refrain from repeating or continuing the act or practice, to redress loss or damage suffered by the complainant (including humiliation or injury to the complainant's feelings), and to pay compensation not exceeding $100,000 for loss or damage.[801]
- In Queensland, QCAT has the power to order that the respondent not repeat or continue a practice, must engage in a stated reasonable act or practice to compensate for loss or damages suffered, apologise, or make an award of damages not exceeding $100,000 for loss or damages, including for any injury to the complainant's feelings or humiliation suffered.[802]

8.2.30 As in the federal jurisdiction, there is a limited right for parties to appeal privacy decisions by State tribunals to the relevant Supreme Court on a point of law.[803]

---

[793] Privacy Act Review Report 2022 252 and citing *Australian Information Commissioner v Facebook Inc* [2020] FCA 531, *Australian Information Commissioner v Facebook Inc (No 2)* [2020] FCA 1307.
[794] *Privacy Act 1988* (Cth) s 80W.
[795] *Privacy Act 1988* (Cth) s 80V.
[796] OAIC, *Guide to Privacy Regulatory Action* (Guidance Document, January 2023) ch 4 [4.18].
[797] Ibid ch 4.
[798] *Privacy Act 1988* (Cth) s 80W; *Regulatory Powers (Standard Provisions) Act 2014* (Cth) s 121.
[799] *Privacy and Personal Information Protection Act 1998* (NSW) s 55(2).
[800] *Privacy and Personal Information Protection Act 1998* (NSW) s 55.
[801] *Privacy and Data Protection Act 2014* (Vic) s 77(1).
[802] *Information Privacy Act 2009* (Qld) s 178. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) amends the provisions in relation to how QCAT may dispose of a complaint (not yet commenced).
[803] For example, *Civil and Administrative Tribunal Act 2013* (NSW) s 83; *Civil and Administrative Tribunal Act 1998* (Vic), s 148; *Civil and Administrative Tribunal Act 2009* (Qld) s 149.

8.2.31 Offences are created in State and Territory legislation. For example, in NSW, Queensland, and Victoria, offences are created predominantly for interference with the duties of the regulatory body (including in relation to investigations) and misconduct by the regulator's office or staff.[804]

8.2.32 The Victorian legislation creates an additional enforcement option not found in legislation in other jurisdictions. This gives the VIC the option to conduct an investigation for the purpose of serving a compliance notice for a serious, flagrant, or repeated breach of a privacy principle or certain other contraventions.[805] The VIC may become aware of issues or allegations of non-compliance through complaints or inquiries from the public or Members of Parliament, information from an informant, publicly available information (such as the media), internal or external referrals, or certain other means.[806] Failure to comply with a notice will incur a penalty and is an indictable offence.[807] Individuals and organisations have a right to seek review of a decision to serve a compliance notice.[808]

8.3 The Commonwealth Privacy Act Review

8.3.1 The Privacy Act Review considered whether existing Privacy Act enforcement mechanisms were adequate in light of 'the scale and sophistication of the use of personal information by APP entities'.[809] It sought submissions on a proposal to create a direct right of action, whereby individuals or groups of individuals could initiate action directly in the Federal Court or Federal Circuit and Family Court of Australia for remedies for loss or damage.[810]

8.3.2 The Review observed that there was broad support for a direct right of action among submitters, on the basis that it would give individuals greater control over their information and incentivise compliance with the Privacy Act,[811] although some raised concerns about burdening the courts and causing adverse impacts on business.[812] The Review also observed that, unlike State and Territory tribunals, the AAT cannot exercise judicial power in its review of the Commissioner's decisions and, on that basis, would not be an appropriate forum for a direct right of action.[813]

8.3.3 The Review ultimately recommended the introduction of a direct right of action that would enable complainants to seek damages or other remedies for loss or damage (including injury to feelings and humiliation) in relation to interference with privacy.[814] The Review explained that this 'would be an important measure to enhance individuals' control of their personal information, and reflect current community expectations', as well as being consistent with rights available under overseas data

[804] See *Privacy and Data Protection Act 2014* (Vic) ss 82, 83E, 83H, 120, 121, 122; *Information Privacy Act 2009* (Qld) Ch 6, Pt 2; *Privacy and Personal Information Protection Act 1998* (NSW) Pt 8. Note amendments in *Information Privacy and Other Legislation Amendment Act 2023* (Qld) (not yet commenced).
[805] *Privacy and Data Protection Act 2014* (Vic) s 78.
[806] Office of the Victorian Information Commissioner, *Regulatory Action Policy* (Web Page, 12 October 2022) <https://ovic.vic.gov.au/regulatory-action/regulatory-action-policy/>.
[807] *Privacy and Data Protection Act 2014* (Vic) s 82.
[808] *Privacy and Data Protection Act 2014* (Vic) s 83.
[809] Privacy Act Review Report 2022 252.
[810] Ibid 275.
[811] Ibid 272.
[812] See ibid 273.
[813] Ibid 275.
[814] Ibid Proposal 26.1.

protection laws.[815] The Government agreed in-principle with this proposal, stating that the right 'would be an important measure to enhance individuals' control over their personal information'.[816]

8.3.4 In order to mitigate the impact of such a reform on court resources, the Review proposed a 'gateway' model, wherein complainants must first complain to the Commissioner (or other complaint-handling body) to have the complaint assessed for conciliation. The complainant could seek the leave of the court in circumstances where the Commissioner determined that conciliation was unsuitable or had terminated the matter, where conciliation had failed, or where the complainant chose not to pursue conciliation at all.[817]

8.3.5 The Review also recommended that a range of changes be made to the civil penalty provisions in the Privacy Act for the purpose of 'better targeted regulatory responses' and to incentivise improved compliance.[818] The Review concluded that the lack of civil penalties for interferences with privacy that are not serious and/or repeated was 'a gap in the regulatory framework'[819] and proposed introducing:

- 'a new low-level civil penalty provision for specific administrative breaches of the Act and the APPs' with attached powers for the Commissioner to issue infringement notices (as an alternative to litigation) and set penalties;[820] and
- 'a new mid-tier civil penalty provision to cover interferences with privacy without a "serious" element, excluding the new low-level civil penalty provision', and which would provide for 'penalties high enough to ensure deterrence'.[821]

8.3.6 The Government agreed that low-level and mid-tier civil penalty provisions should be introduced.[822]

8.3.7 The Review observed that there has been no judicial guidance on the interpretation of the civil penalty provisions applying to serious or repeated breaches and proposed that the provision be amended to remove the word 'repeated' and clarify what amounts to a 'serious' interference, with supporting guidance developed by the OAIC.[823] The Government agreed with this proposal.[824]

---

[815] Privacy Act Review Report 2022 273. The Review also sought submissions on a proposal for the establishment of a distinct role of Federal Privacy Ombudsman to handle complaints but did not make such a proposal in its Final Report: ibid 268–269.
[816] Government Response 19.
[817] Privacy Act Review Report 2022 272, 275. The ACCC made similar recommendations concerning damages for financial and non-financial harm suffered as a result of interference with privacy in the DPI Report: ACCC, *Digital Platforms Inquiry* 472–473.
[818] Privacy Act Review Report 2022 253–254.
[819] Ibid 254.
[820] Ibid Recommendation 25.1 and 255. The Review suggested that low-level penalties would be suitable for breaches such as a breach of the requirement in APP1.3 to have a clearly expressed and up-to-date privacy policy and the requirement in APP2.1 to give individuals the option of not identifying themselves: ibid 256.
[821] Ibid Recommendation 25.1 and 255.
[822] Government Response 20.
[823] Privacy Act Review Report 2022 Recommendation 25.2 and 258. The Review suggested that a serious interference may include:
- 'those involving 'sensitive information' or other information of a sensitive nature;
- 'those adversely affecting large groups of individuals';
- 'those impacting people experiencing vulnerability';
- 'repeated breaches';
- 'wilful misconduct'; and
- 'serious failures to take proper steps to protect personal data': ibid Recommendation 25.2.

[824] Government Response 20.

8.3.8 The Review also proposed reforms, with which the Government agreed,[825] that would enable the Commissioner to be more proactive in relation to assessments, investigations and inquiries by:

- enhancing its powers of investigation of civil penalty provisions;[826]
- introducing a new power for the Commissioner to undertake public inquiries and reviews on the approval or direction of the Attorney-General (in relation to systemic issues or issues in specific industry sectors);[827] and
- empowering the Commissioner to make declarations requiring the entity to identify, mitigate (and not just redress) loss or damage, and in relation to both actual and reasonably foreseeable loss or damage.[828]

8.3.9 The Review observed that the Federal Court can impose a pecuniary penalty, but not an order for compensation, upon a finding that an entity has engaged in serious and/or repeated breaches in contravention of Section 13G of the Privacy Act.[829] It proposed, and the Government agreed, that it would be appropriate for the Privacy Act to be amended to give the Federal Court and Federal Circuit and Family Court of Australia the power to make 'any order it sees fit', following such a finding.[830]

8.3.10 The Review acknowledged the importance of the OAIC being adequately resourced to carry out its regulatory functions, including enforcement functions, effectively. It recommended further consideration be given to the introduction of an industry funding model for the OAIC,[831] a contingency litigation fund (similar to the one available to the Australian Competition and Consumer Commission ('ACCC')) to fund litigation costs orders made against it, and an enforcement special account (such as those held by Australian Prudential Regulation Authority ('APRA') and the Australian Securities and Investments Commission ('ASIC')) to fund high-cost litigation.[832] The Government agreed with this proposal in-principle.[833]

8.3.11 The Review recommended that the OAIC's annual reporting obligations be adjusted to require the OAIC to report on all complaint outcomes, on the basis that this would provide greater transparency (including in relation to the grounds on which complaints are dismissed).[834] The Government agreed with this proposal.[835] The Review made several other recommendations to enhance the OAIC's capacity to exercise its complaint handling and enforcement functions, including a strategic internal organisational review.[836]

[825] Government Response 20.
[826] Privacy Act Review Report 2022 Recommendation 25.3.
[827] Ibid Recommendation 25.4.
[828] Ibid Recommendation 25.5. The Review recommended that OAIC guidance should be developed to guide entities on how to achieve this.
[829] Ibid 264.
[830] Ibid Recommendation 25.6; Government Response 20.
[831] Privacy Act Review Report 2022 Recommendation 25.7.
[832] Ibid Recommendation 25.8.
[833] Government Response 20.
[834] Privacy Act Review Report 2022 Recommendation 25.9.
[835] Government Response 20.
[836] Privacy Act Review Report 2022 Recommendation 25.10. The Government agreed with this proposal: Government Response 20.

8.4 Consultation

8.4.1 The TLRI posed four questions in the Issues Paper relating to complaints, remedies, and other enforcement action under the PIPA:

> How effective is the current complaints process in enforcing obligations under the PIPA?[837]
>
> Should consideration be given to amending the PIPA to include provision for an individual to appeal or seek review if they are dissatisfied with the actions or recommendations of the Ombudsman in investigations of privacy complaints?[838]
>
> What other remedies should be available to individuals affected by a breach of the PIPA?[839]
>
> Are there other forms of enforcement action that should be introduced?[840]

8.4.2 The Tasmanian Ombudsman was critical of the approach to enforcement and remedies in the PIPA, stating that:

> The absence of remedies or enforcement provisions in the event of a breach is an unusual feature of the Act.… In practice I have found it to be quite ineffective because, although I can make recommendations, I am unable to achieve outcomes that might satisfy a complainant and offer some sort of recompense for damage suffered.

8.4.3 Meg Webb MLC expressed the view that it is difficult to assess the quality of the current complaints process under the PIPA due to a lack of data on:

- whether the Ombudsman's recommendations are acted upon and effectively implemented; and
- whether the recommendations have a long-term educative influence on personal information custodians subject to complaints.[841]

8.4.4 TasCOSS and Meg Webb MLC also expressed support for reforms to empower the Ombudsman to initiate own-motion investigations, with Ms Webb arguing that this would add rigour to PIPA compliance in general.[842]

8.4.5 The Tasmanian Ombudsman indicated support for amendments to the PIPA to make Ombudsman decisions reviewable by TasCAT. TasCOSS also expressed support for the creation of avenues of appeal of the Ombudsman's decisions by an independent tribunal. Meg Webb MLC observed that appeals processes are available in other Australian jurisdictions and submitted that understanding of, and confidence in, appeals and redress mechanisms is an element of informed consent.

8.4.6 As noted elsewhere in this Report, the Tasmanian Ombudsman suggested a 'wholesale review' of the PIPA. The Ombudsman submitted that this should include 'serious consideration [as] to

[837] Issues Paper Part 2, Question 2.10.
[838] Ibid Part 2, Question 2.11.
[839] Ibid Part 2, Question 2.12.
[840] Issues Paper Part 2, Question 2.13.
[841] Submission 8 (Meg Webb MLC).
[842] Submission 8 (Meg Webb MLC) 12; see also Submission 11 (TasCOSS). The TLRI notes that the Ombudsman does appear to have this power: see [8.2.10] above.

whether a discrete body should be established to administer the Act, investigate potential breaches and take enforcement action'.

8.4.7 The Ombudsman emphasised that the implementation of reforms to insert penalty and compensation provisions, and to make the Ombudsman's decisions reviewable by TasCAT, would be 'impossible' with the current resourcing (staffing) of the Ombudsman's office.[843] TasCOSS also strongly recommended that any reforms to the Ombudsman's powers should be accompanied by additional funding and resourcing.[844]

8.4.8 Meg Webb MLC submitted that consideration should be given to amending the PIPA to provide for compensation for a breach of a PIPP, consistent with legislation in Queensland, NSW, and Victoria.[845] TasCOSS expressed support for reforms to empower the Tasmanian Ombudsman to award compensation for privacy breaches. Youth Law Australia called for reparation (including compensation) for breaches of the privacy of children and young people.[846]

8.4.9 In terms of other types of enforcement action, Meg Webb MLC submitted that the inclusion in the PIPA of civil penalty provisions, such as those found in the Commonwealth Privacy Act, should be investigated. TasCOSS suggested that the Ombudsman should have 'broader enforcement powers', including the power to make orders to mitigate potential privacy risks, to delete personal information collected unlawfully or inappropriately, to seek an injunction at various stages of a complaints process, and to impose penalties.

8.4.10 Alex Kendall of Phillips Taglieri Barristers & Solicitors submitted that the PIPA should be amended to permit a suitable court or tribunal to make an order requiring a personal information custodian to provide access or produce an individual's personal information.[847] As discussed in more detail in [6.5.6] and following, the Tasmanian Ombudsman expressed support for the PIPA to be amended to either clarify the relationship between PIPP 6(1) and Section 13 of the *Right to Information Act 2009* (Tas) ('RTI Act') (to make it a deeming provision and hence make review rights and prescribed timeframes under the RTI Act applicable), or to prescribe timeframes and create a separate right to seek external review for a failure to provide access and to seek redress for a delay in doing so. This is consistent with the Commission of Inquiry into the Tasmanian Government's Responses to Child Sexual Abuse in Institutional Settings ('CoI') recommendation that consideration be given to reforming the PIPA and RTI Act to 'streamline the interface between [the Acts]'.[848]

8.4.11 TasCOSS submitted that independent oversight of police complaints is required to ensure the appropriate exercise of powers and enhance public confidence in the police.[849] This submitter noted calls by some Victorian community organisations for the introduction of an independent police ombudsman to respond to complaints, achieve timely and fair outcomes, and promote systemic change, and indicated its support for the creation of a similar entity in Tasmania.[850] This issue is discussed further at [10.2] and following of this Report.

[843] Submission 4 (Tasmanian Ombudsman) 2.
[844] Submission 11 (TasCOSS).
[845] Submission 8 (Meg Webb MLC).
[846] Submission 12 (Youth Law Australia).
[847] Submission 1 (Alex Kendall).
[848] CoI Report Recommendation 17.8(2).
[849] Submission 11 (TasCOSS).
[850] Ibid.

8.4.12 Youth Law Australia cited the United Nations Committee on the Rights of Children ('CRC') in calling for appeal options and remedies for breaches of privacy rights that are accessible and appropriate for children and young people. According to the CRC:

> For rights to have meaning, effective remedies must be available to redress violations … States need to give particular attention to ensuring that there are effective, child-sensitive procedures available to children and their representatives. These should include the provision of child-friendly information, advice, advocacy, including support for self-advocacy, and access to independent complaints procedures and to the courts with necessary legal and other assistance. Where rights are found to have been breached, there should be appropriate reparation, including compensation …[851]

8.5 The TLRI's view

8.5.1 In the TLRI's view, there is considerable scope to strengthen the PIPA complaints process, and to make provision for remedies for breaches of the PIPA, in order to enhance privacy protections for individuals and foster personal information custodians' compliance with the PIPA.

8.5.2 The changes recommended in this Part will have considerable resource implications. The TLRI recommends, consistent with the Tasmanian Ombudsman's submission, that consideration be given to the most appropriate form that a body responsible for broadened enforcement and compliance functions should take, and to ensuring adequate resourcing for that body.

8.5.3 In terms of the complaints process, the TLRI notes that the Commonwealth Privacy Act and privacy legislation in Victoria, Queensland, and NSW requires the relevant commissioner to consider the appropriateness of conciliation when dealing with a complaint. The Ombudsman is not so obliged under the PIPA. The TLRI did not seek, and did not receive, submissions directly on this point. The TLRI recommends further consideration be given to the introduction of a similar requirement in the PIPA, on the basis that it may foster timely and efficient resolution of complaints.

8.5.4 Several submissions in response to the Issues Paper queried the effectiveness of the existing PIPA complaints process and its accessibility to all Tasmanians, such as children and young people. The TLRI recommends that any changes made to the complaints and review process arising from this Review needs to consider the accessibility and availability of those mechanisms to all in the community.

8.5.5 The TLRI observes that privacy complaints processes in the other Australian jurisdictions discussed in this Part are accompanied by:

- avenues to appeal initial decisions about complaints to a tribunal;
- powers for privacy complaints to be referred to a tribunal; and
- powers for either the initial decision-maker (at the Commonwealth level) or the tribunal (in Victoria, Queensland, and NSW) to make one or more of a range of determinations or orders by way of remedy.

8.5.6 The TLRI further observes that the CoI recommended in its final report that reforms to the PIPA and RTI Act be considered to 'strengthen and streamline internal and external review processes

[851] Submission 12 (Youth Law Australia) quoting Committee on the Rights of the Child, General Comment No 5 (2003) *General Measures of Implementation of the Convention on the Rights of the Child* (arts 4, 42 and 44, para 6) UN Doc CRC/GC/2003/527.

… with a focus on options to enforce decisions of the Ombudsman and to apply for review by the Tasmanian Civil and Administrative Tribunal'.[852]

8.5.7 The TLRI recommends that decisions of the Tasmanian Ombudsman (or other complaint handling body) about PIPA complaints should be reviewable by TasCAT, consistent with the approach in Victoria, NSW, and Queensland. In addition, there should be provision for the matter to be referred to TasCAT if resolution of the complaint cannot be achieved through mediation, as exists in Queensland and Victoria.[853]

8.5.8 The TLRI further considers that TasCAT should be empowered to make one or more of a range of orders against a personal information custodian if part or all of a PIPA complaint is proven, such as orders that entities act, or refrain from acting, so as to comply with a privacy principle, change their practices, or remedy loss or damage, including through payment of compensation. This is consistent with the approach taken in Victoria, Queensland, and NSW.

8.5.9 The TLRI notes the Privacy Act Review's recommendations relating to expanding the scope of determinations (orders) available in the Commonwealth jurisdiction, by enabling the Commissioner to make orders requiring the respondent to identify and mitigate loss or damage, and to make orders relating to both actual and reasonably foreseeable loss or damage.[854] In its submission in response to the Issues Paper to the present project, TasCOSS made a similar suggestion that orders to mitigate potential privacy risks be available. The TLRI considers that it may also be appropriate to make orders of this nature available to TasCAT, because they would provide greater protection or remediation of individuals' privacy and stronger incentives for custodians to comply with the PIPPs.

8.5.10 The TLRI considers that it may also be appropriate to create a scheme in the PIPA setting out offences for certain conduct (as exists in New South Wales, Victoria, and Queensland) and/or a civil penalty regime (as exists in the Privacy Act) in order to foster compliance and appropriately penalise serious breaches of the PIPPs.

8.5.11 The TLRI notes that the Privacy Act Review proposed the introduction of a tiered system of civil penalties for 'low', 'mid', and 'serious' breaches for this purpose. Under the proposed reforms, the OAIC would be empowered to take civil penalty proceedings in the Federal Court or Federal Circuit and Family Court of Australia.[855] This will be a more comprehensive regime than currently exists at the Commonwealth level. The TLRI considers that further consideration should be given to the appropriate form that a civil penalty scheme should take in Tasmania, if any.

8.5.12 The TLRI observes that other enforcement mechanisms, including injunctions and enforceable undertakings, are available in other jurisdictions. One submission (from TasCOSS) supported empowering the Ombudsman to seek injunctions 'at various stages of a complaints process'. The TLRI considers that consideration should be given to the appropriate scope of enforcement mechanisms available to the Ombudsman or other administering body.

8.5.13 The TLRI did not seek, and did not receive, submissions on whether a direct right of action to seek compensation or other orders from Tasmanian courts for breaches of the PIPA should be introduced. The TLRI notes the recommendation of the Privacy Act Review for the introduction of such a direct right of action at the Federal level, and the Review's conclusion that such a right of action

[852] CoI Report Recommendation 17.8(2).
[853] See *Information Privacy Act 2009* (Qld) Ch 5 Pt 4; *Privacy and Data Protection Act 2014* (Vic) s 66.
[854] Privacy Act Review Report 2022 Recommendation 25.5. The Review recommended that OAIC guidance should be developed to guide entities on how to achieve this.
[855] Ibid 253–255.

would be justified in light of the 'potential benefits for individuals and for compliance with the Act'[856] in giving individuals greater control over their private information and in creating another incentive for regulated entities to comply with the Privacy Act. However, the TLRI also notes that the Privacy Act Review's recommendation was underpinned, in part, by the AAT's lack of judicial powers, in contrast to the powers of the State and Territory tribunals (see [8.3.2]).[857] On this basis, the TLRI does not make any recommendations about the introduction of a direct right of action to seek compensation or other orders from Tasmanian courts. The TLRI does recommend that the enforcement provisions in PIPA be strengthened to provide for orders that can be made by TasCAT, in the event that a complaint is proven. Judicial review of TasCAT decisions would then be available through the courts.

8.5.14 The TLRI observes that regulatory bodies in some Australian jurisdictions are empowered to conduct investigations on their own initiative in some circumstances. For example, the VIC can investigate potential serious, flagrant, or repeated breaches of the Victorian Act for the purpose of issuing a compliance notice, while the NSWPC can conduct inquiries and investigations into privacy related matters as they consider appropriate (see [8.2.21]). It is also noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) will provide the Information Commissioner with the power to conduct own-motion investigations once it has been commenced. The TLRI further notes that the Privacy Act Review also recommended broadening the Commissioner's powers to enable it to conduct public inquiries and reviews regarding systemic issues.

8.5.15 In the TLRI's view, the Tasmanian Ombudsman (or other complaints-handling body) should clearly be provided with a legislative power to conduct investigations into breaches of the PIPPs, regardless of whether a complaint has been received. If a civil penalty regime is introduced, then the PIPA should enable the Ombudsman to seek penalties if such an investigation establishes that there has been a breach. Alternatively, consideration could be given to creating a compliance notice scheme as exists in Victoria. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) will create a mandatory data breach scheme once it is commenced.[858]

8.6 Recommendations

Recommendation 47: Consideration should be given to:

- the most appropriate form that a body responsible for broadened enforcement and compliance functions under the PIPA should take; and
- ensuring adequate resourcing for that body.

Recommendation 48: Consideration should be given to the introduction of a requirement for the Ombudsman (or other complaints-handling body) to consider the appropriateness of conciliation when dealing with a complaint. There should also be jurisdiction for TasCAT to hear a complaint, if the Ombudsman (or other complaints-handling body) decides that it is not reasonably possible that a complaint be conciliated successfully.

Recommendation 49: Community consultation should be undertaken to ensure that changes to complaints and review processes under the PIPA are available and accessible to all in the community.

Recommendation 50: Decisions of the Ombudsman (or other complaints-handling body) in relation to PIPA complaints should be reviewable by TasCAT.

[856] Privacy Act Review Report 2022 274.
[857] Ibid 275.
[858] See [8.12.9] below.

Recommendation 51: TasCAT should be empowered to make appropriate orders against personal information custodians, where all or part of a PIPA complaint has been proven.

Recommendation 52: Consideration should be given to strengthening the enforcement regime through:

- the creation of offences for certain conduct;
- a civil penalty regime; and/or
- the creation of additional enforcement mechanisms, such as injunctions and enforceable undertakings.

Guidance can be sought from the provision in other Australian jurisdictions as to the scope of the regimes.

Recommendation 53: The power of the Ombudsman (or other complaints-handling body) to conduct investigations into breaches of the PIPPs, regardless of whether a complaint has been received, should be clarified.

8.7 Other regulatory action

The Tasmanian position

8.7.1 Two additional forms of regulatory action currently absent from the PIPA are available in Commonwealth and/or other State and Territory legislation: privacy codes and privacy impact assessments.

The position in other jurisdictions

8.7.2 Commonwealth, NSW, and Victorian privacy legislation provide for mechanisms to develop and approve 'privacy codes', or codes of practices about information privacy.[859]

8.7.3 At the Commonwealth level, an 'APP code' does not replace the APPs but operates in addition to the APP requirements discussed in Parts 4–7 of this Report.[860] According to the OAIC, such codes augment the APPs and provide greater transparency on how personal information is handled. A breach of a code generally has the same legal effect as a breach of the privacy principles.[861]

8.7.4 Under the Privacy Act, APP codes may be developed by entities (termed 'APP code developers'), either on their own initiative or upon request by the Australian Information Commissioner.[862] The Commissioner may only develop an APP code where an APP code developer has not complied with a request to develop a code, or the Commissioner has decided not to register an APP code that has been developed as requested.[863] The codes set out how one or more APPs are to be applied or complied with, and may also impose additional requirements.[864] The Commissioner registers

[859] *Privacy Act 1988* (Cth) s 26C; OAIC, *APP Guidelines* [B.126].
[860] OAIC, *APP Guidelines* [B.128].
[861] *Privacy Act 1988* (Cth) s 13(1)(b); OAIC, *APP Guidelines* [B.127].
[862] *Privacy Act 1988* (Cth) s 26E.
[863] *Privacy Act 1988* (Cth) s 26G.
[864] *Privacy Act 1988* (Cth) s 26C.

approved codes on a Codes Register.[865] As at 1 February 2024, there were three registered privacy codes in force.[866]

8.7.5 One such code is the Privacy (Australian Government Agencies – Governance) APP Code 2017, which 'prescribes the steps that Australian government agencies must take to comply with APP 1.2'; that is, to take reasonable steps to implement practices, procedures, and systems to ensure compliance with the APPs (see [7.2.6] and following for a detailed discussion).

8.7.6 One requirement imposed by 2017 APP Code is that agencies must complete a privacy impact assessment where they undertake 'high risk privacy projects'.[867] Section 33D of the Privacy Act also empowers the Commissioner to direct government agencies to undertake a privacy impact assessment.[868] The Privacy Act defines 'privacy impact assessment' as 'a written assessment of an activity or function that … identifies the impact the activity or function might have on the privacy of individuals; and … sets out recommendations for managing, minimising, or eliminating that impact'.[869] Agencies must maintain a register of their privacy impact assessments and publish them on their websites.[870]

8.7.7 Legislation in other Australian jurisdictions also provides for the development of privacy codes of practice, although the purpose and effect of these differ from those made under the Privacy Act. For example, in Victoria and NSW, codes of practice can *modify* the application of one or more of the applicable privacy principles in relation to specified information, a specific public sector body, or a specific activity (or classes thereof).[871]

8.7.8 The Victorian legislation specifies that a code of practice may only prescribe standards that are at least as stringent as the standards prescribed in the information privacy principle.[872] In addition to modifying the application of one or more privacy principles, Victorian codes of practice can prescribe how one or more of the principles should be applied or complied with, set guidelines on charging, and prescribe procedures for complaints and remedies, among other things.[873] Public sector organisations can discharge their duty to comply with the privacy principles by complying with an approved code of practice.[874] Contraventions of a code are taken to be contraventions of the privacy principles and can be dealt with as provided by the code and the legislation.[875]

8.7.9 Conversely, the NSW legislation specifies that requirements imposed under a code must not impose requirements that are more stringent than the information privacy principles.[876] Such a code may specify different requirements from the requirements set out in the principles, exempt any activity or conduct from compliance with any principle, specify how one or more principles are to be applied

[865] *Privacy Act 1988* (Cth) ss 26F–26H.
[866] Privacy (Credit Reporting) Code 2014; Privacy (Australian Government Agencies – Governance) APP Code 2017 (Cth); Privacy (Market and Social Research) Code 2021: see OAIC, *Privacy Codes Register* (2020) <https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/>.
[867] APP Code 2017 s 12.
[868] *Privacy Act 1988* (Cth) s 33D.
[869] OAIC, *Guide to Undertaking Privacy Impact Assessments* (Guidance Document, May 2020) <https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments>.
[870] APP Code 2017 ss 13, 15(1).
[871] *Privacy and Personal Information Protection Act 1998* (NSW) s 30(1); *Privacy and Data Protection Act 2014* (Vic) s 21. Codes may also be made under the Victorian Act in relation to a specified industry, profession, or calling: *Privacy and Data Protection Act 2014* (Vic) s 21(3).
[872] *Privacy and Data Protection Act 2014* (Vic) 21(2)(a).
[873] *Privacy and Data Protection Act 2014* (Vic) s 21(2), (4).
[874] *Privacy and Data Protection Act 2014* (Vic) s 21(1).
[875] *Privacy and Data Protection Act 2014* (Vic) s 24.
[876] *Privacy and Personal Information Protection Act 1998* (NSW) s 29(7)(b).

or followed, and exempt an agency or class of agency from the requirement to comply with one or more principles altogether.[877] Codes are binding on agencies subject to them, and complaints can be made for breaches of a code under the same provisions that address complaints for breaches of the privacy principles.[878]

8.7.10 The process for developing privacy codes is similar in Victoria and NSW. A public sector body bound by the legislation may initiate the development of a code and the relevant commissioner must be involved.[879] In NSW, the Minister is empowered to decide whether a code should be made;[880] in Victoria, the Information Commissioner may advise the Minister to recommend the making of the code to the Governor in Council if certain requirements are met.[881] The *Health Records Information Privacy Act 2002* (NSW) makes similar provision for the making of Health Privacy Codes of Practice to modify the application of one of more of the Health Privacy Principles.[882]

8.7.11 The Office of the Victorian Information Commissioner ('OVIC') has reported that no organisations have applied for approval of a code of conduct under the Victorian legislation.[883] The NSWPC lists 17 privacy codes of practice, and 5 health privacy codes of practice, that have been approved and gazetted.[884] These include, for example:

- Privacy Code of Practice for the Judicial Commission of NSW (22 October 2021)
- Privacy Code of Practice for Local Government revised (20 December 2019)
- Privacy Code of Practice for the Office of the Director of Public Prosecutions (30 June 2000)
- Health Privacy Code of Practice for the Public Service Commission (28 September 2018)
- Privacy Code of Practice for NSW Health (30 June 2000)

8.7.12 State legislation does not oblige regulated entities to undertake privacy impact assessments, although bodies such as the VIC, the NSWPC, and the QIC recommend that such assessments be completed to support compliance with privacy principles, and have published guidance to support the conduct of these assessments.[885]

---

[877] *Privacy and Personal Information Protection Act 1998* (NSW) s 30(2).
[878] *Privacy and Personal Information Protection Act 1998* (NSW) s 32.
[879] *Privacy and Personal Information Protection Act 1998* (NSW) ss 31(1), 31(2); *Privacy and Data Protection Act 2014* (Vic) s 22(1). The NSW legislation specifies that requirements imposed under a code must not impose requirements that are more stringent than the information privacy principles (s 29(7)(b)), while the Victorian legislation specifies that a code of practice may only prescribe standards that are at least as stringent as the standards prescribed in the information privacy principle (s 21(2)(a)).
[880] *Privacy and Personal Information Protection Act 1998* (NSW) s 31(4).
[881] *Privacy and Data Protection Act 2014* (Vic) ss 22(2), (3).
[882] *Health Records Information Privacy Act 2002* (NSW) Pt 5.
[883] OVIC, *The PDP Act – A Deep Dive* (Web Page) <https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-officer-toolkit/the-pdp-act-a-deep-dive/>.
[884] IPCNSW, Codes of Practice (Web Page, 2023) <https://www.ipc.nsw.gov.au/privacy/nsw-privacy-laws/privacy-codes-practice>.
[885] OVIC, *Privacy Impact Assessment Guide* https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-impact-assessment/ ; Information and Privacy Commission New South Wales, *A Guide to Privacy Impact Assessments* (Updated May 2020) <https://www.ipc.nsw.gov.au/sites/default/files/2021-03/Guide_to_Privacy_Impact_Assessments_May_2020.pdf>; Office of the Information Commissioner Queensland, *Undertaking a Privacy Impact Assessment* (Web Page, 7 March 2022) <https://www.oic.qld.gov.au/guidelines/for-government/guidelines-privacy-principles/privacy-compliance/overview-privacy-impact-assessment-process/undertaking-a-privacy-impact-assessment>

8.7.13 In Queensland, it is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) contains provisions in relation to a QPP code.[886]

8.8 The Commonwealth Privacy Act Review

8.8.1 According to the Privacy Act Review, the OAIC made a submission that the Privacy Act's limitations on when the Commissioner can make an APP code were affecting the efficacy of the code-making powers. The Review consequently proposed that the Commissioner be empowered to make APP codes where the Attorney-General has directed or approved the making of a code in circumstances where: (a) it is in the public interest for a code to be developed; and (b) there is unlikely to be an appropriate industry representative to develop the code.[887]

8.8.2 In response to submissions that stronger consultation requirements would be necessary to ensure adequate industry involvement in the development of APP codes, the Review further proposed that codes must be made available for public consultation for at least 40 days and that the Commissioner must be able to consult any person the Commissioner considers appropriate, and consider matters specified in relevant guidelines, at any stage during the process.[888]

8.8.3 The Review further proposed the creation of a new power for the Commissioner to issue temporary APP codes for a maximum period of 12 months, either as directed by the Attorney-General or with the Attorney-General's approval, where the code is urgently required and its issuance is in the public interest.[889] This proposal addressed concerns about the potentially lengthy process of APP code development which makes it difficult to address urgent situations (such as the COVID-19 pandemic).[890]

8.8.4 The Government agreed with each of these proposals.[891]

8.8.5 The Privacy Act Review also contemplated the development of several new APP codes. It proposed that a Children's Online Privacy Code be developed in consultation with a range of stakeholders,[892] and that further guidance on standardisation of templates, layouts, terminology, and icons used for privacy policies and collection notices online may be appropriately housed in an APP code, such as an 'Online Privacy Code' (see [5.4.40]).[893]

8.8.6 The Review also suggested that consideration be given to the development of codes of practice to 'clarify obligations regarding collection, use and disclosure of personal and sensitive information', if enhanced privacy protections for employee data are extended to private sector employees (see [4.13.1] and following).[894]

8.8.7 As discussed at [7.3], the Privacy Act Review proposed—and the Government agreed in-principle—that the obligation on agencies to conduct privacy impact assessments in relation to high risk privacy projects be moved from the APP code to the Privacy Act itself, and extended to apply to all APP entities in relation to all activities that are 'likely to have a significant impact on the privacy of

[886] See discussion in Explanatory Memorandum 18–20.
[887] Privacy Act Review Report 2022 Proposal 5.1.
[888] Ibid.
[889] Ibid Proposal 5.2.
[890] Ibid 49–50.
[891] Government Response 15.
[892] Privacy Act Review Report 2022 Proposal 16.5 (see also Proposal 16.3); Government Response 13.
[893] Ibid Proposal 10.3 and 99–100.
[894] Ibid Proposal 7.1.

individuals'.[895] The Review proposed that assessments should be undertaken prior to the high-risk activity being undertaken, and that entities should be required to produce assessments to the OAIC upon request.[896] The Review also proposed the development of OAIC guidance to assist entities to determine whether a privacy impact assessment is required, and contemplated the inclusion of specific high-risk practices in the Privacy Act.[897]

8.9 Consultation

8.9.1 The TLRI Issues Paper invited responses to the following question:

> Should consideration be given to the development of privacy codes by amendment to the PIPA or by providing for similar rules to be made in delegated legislation?[898]

8.9.2 One submission addressed this question. Meg Webb MLC expressed support for the amendment of the PIPA to provide mechanisms and processes for the development of binding privacy codes, a breach of which should have the same legal effect as a breach of the PIPPs at a minimum.[899]

8.10 The TLRI's view

8.10.1 Existing regulatory schemes in other jurisdictions, and the recommendations of the Commonwealth Privacy Act Review, suggest that amendments to the Tasmanian PIPA to provide for the development of privacy codes, or to provide for similar rules to be made in delegated legislation, could have a number of advantages in terms of:

- transparency for individuals, because codes may clarify how particular information is handled, or how particular agencies or classes of agencies handle information (elements of which are found in the equivalent schemes in the Privacy Act and Victorian and NSW legislation);
- flexibility for agencies on PIPP compliance, where codes enable agencies to seek modification of the requirements that apply to them and even exemption from certain requirements (as in the NSW legislation); and/or
- agility for the Ombudsman or other administering body in responding promptly to emerging or urgent privacy issues, where codes can be developed at that body's instigation and on a temporary basis where it is in the public interest (as proposed by the Commonwealth Privacy Act Review).

8.10.2 For these reasons, the TLRI recommends that a privacy codes function be introduced in the PIPA. The TLRI observes that there are significant differences between the scope and nature of privacy codes of practice that can be made under Commonwealth, Victorian, and NSW legislation, and in the extent to which these schemes have been utilised. In light of the limited submissions received on this issue, further consideration should be given to the precise form this function should take.

8.10.3 The TLRI did not pose a question in the Issues Paper on whether privacy impact assessments should be encouraged or required in certain circumstances under the PIPA. The TLRI observes the

[895] Privacy Act Review Report 2022 Proposal 13.1; Government Response 10.
[896] Ibid Proposal 13.1.
[897] Ibid and see Proposal 13.3.
[898] Issues Paper Part 2, Question 2.14.
[899] Submission 8 (Meg Webb MLC).

Privacy Act Review's recommendations about increasing the use of high risk privacy impact assessments, especially in the context of growing digital privacy risks, and the existing (non-binding) guidance from other state commissioners that recommends and facilitates privacy impact assessments to support regulated entities' compliance with privacy protections.

8.10.4 The TLRI considers that similar privacy impact assessments could be a useful tool for personal information custodians to identify and manage privacy risks associated with their functions and activities.

8.11 Recommendations

Recommendation 54: The PIPA should be amended to enable the creation of privacy codes.

8.12 Mandatory data breach notification

The Tasmanian position

8.12.1 Under Tasmanian law, if a personal information custodian deals with information in a manner that breaches the PIPPs, it is not obliged under the PIPA to inform the Ombudsman or the individual concerned. In contrast, other jurisdictions in Australia and overseas have recently introduced schemes for mandatory reporting of certain breaches.

The position in other jurisdictions

8.12.2 A mandatory data breach notification scheme has operated under Commonwealth privacy law since February 2018.[900] The scheme requires all entities subject to the Privacy Act to investigate and report 'eligible data breaches' to the Commissioner and to the individuals in the information. This is meant to allow affected individuals to take steps to minimise any harm, to encourage entities to better comply with privacy obligations, and to promote transparency of information handling practices.[901] It applies to personal information, tax file number information, and credit information.[902]

8.12.3 'Eligible data breaches' arise when the following three conditions are satisfied:[903]

- there has been unauthorised access to, or disclosure of, personal information or, alternatively, information has been *lost* in circumstances where such access or disclosure is likely to occur;
- a reasonable person would conclude that such access or disclosure is likely to result in serious harm to those individuals related to the information, with degree of harm being determined by reference to a list of factors;[904] and

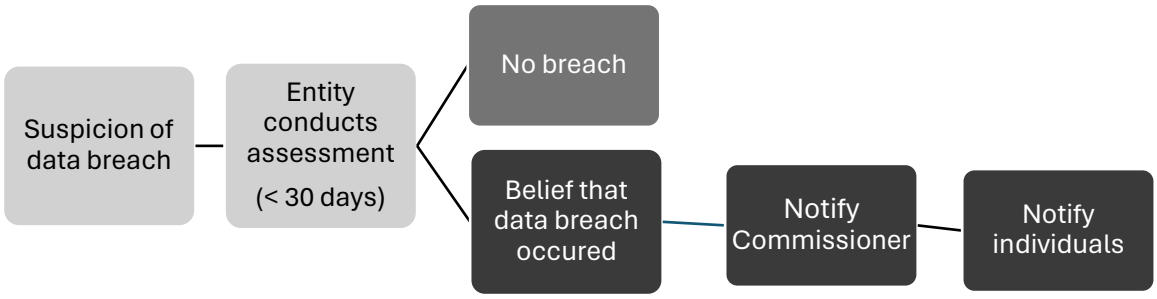
[900] *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth); *Privacy Act* Part IIIC.
[901] Attorney-General's Department, *Privacy Amendment (Notifiable Data Breaches) Bill 2016 Regulation Impact Statement* (Regulation Impact Statement, 11 January 2017) 15.
[902] *Privacy Act 1988* (Cth) s 26WE.
[903] *Privacy Act 1988* (Cth) ss 26WE–26WG.
[904] *Privacy Act 1988* (Cth) s 26WG. This provides that regard should be had to factors such as: the kind(s) of information, the sensitivity of the information, whether the information is protected by security measures, and the persons or kinds of persons who have obtained, or could obtain, the information.

- the entity has not taken remedial action prior to serious harm be caused and, as a result of that action, a reasonable person would conclude that the access or disclosure would not be likely to result in serious harm.[905]

8.12.4 Where an entity reasonably believes that such a breach has occurred, it must, as soon as practicable, prepare a statement and provide a copy to the Commissioner.[906] After notifying the Commissioner, the entity must take reasonable steps to inform the individuals affected, either by communicating directly with them or, where direct communication is not practicable, through general publicity.[907]

8.12.5 If an entity becomes aware of reasonable grounds to *suspect* there has been an eligible data breach, it must investigate to determine whether there are reasonable grounds to *believe* it has occurred and the above process must be followed.[908] The entity must take all reasonable steps to complete this assessment within 30 days.[909] The Privacy Act does establish a process for such assessments—entities develop their own processes.[910]

Figure 8.1 Mandatory eligible data breach notification scheme (simplified)



8.12.6 A failure to meet the Privacy Act's data breach notification requirements constitutes an interference with an individual's privacy, meaning individuals can complain to the Commissioner and the Commissioner's enforcement powers (such as powers to make a determination, accept an enforceable undertaking, and seek an injunction), described above, are available.[911]

8.12.7 On the whole, the obligations under the Commonwealth scheme are less onerous in terms of timeframes than those imposed by the European Union's General Data Protection Regulation 2016/679 ('GDPR'). Generally, the GDPR requires notification of personal data breaches[912] without undue delay

[905] *Privacy Act 1988* (Cth) s 26WF.
[906] *Privacy Act 1988* (Cth) s 26WK.
[907] *Privacy Act 1988* (Cth) s 26WL. The OAIC guidance document on data breaches states that the entities must 'must publish a copy of the statement prepared for the Commissioner on its website, and take reasonable steps to bring its contents to the attention of individuals at risk of serious harm': OAIC, *Data Breach Preparation and Response: A Guide to Managing Data Breaches in Accordance with the Privacy Act 1988 (Cth)* (Guidance Document, July 2019) 48 ('*Data Breach Preparation and Response*').
[908] *Privacy Act 1988* (Cth) s 26WH(1) and (2)(a).
[909] *Privacy Act 1988* (Cth) s 26WH(2)(b).
[910] OAIC, *Data Breach Preparation and Response* 47.
[911] *Privacy Act 1988* (Cth) s 13(4A).
[912] Defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data: see GDPR art 4.

and, where feasible, within 72 hours of the entity having become aware of it.[913] The individuals affected must be informed whenever the breach is likely to result in a high risk to their privacy rights.[914]

8.12.8 In the first 12 months after the scheme was introduced in February 2018, there were 964 mandatory data breach notifications—a 712% increase compared with the previous 12 months, when notification was voluntary.[915] In the most recent reporting period (January to June 2023), there were 409 notifications, with the top 5 sectors notifying data breaches being health service providers, finance, recruitment agencies, legal, accounting and management services, and insurance. Sources of breaches were identified as follows: 70% arose from a malicious or criminal attack; 26% arose from human error; and 4% were due to a system fault.[916]

8.12.9 Australian State and Territory jurisdictions have also begun making moves to implement mandatory data breach notification schemes modelled on the Commonwealth model. The NSW Mandatory Notification of Data Breach ('MNDB') Scheme came into effect on 28 November 2023, following extensive community consultation.[917] In Queensland, a mandatory breach scheme was introduced in the *Information Privacy and Other Legislation Amendment Act 2023* (Qld), which is yet to be commenced.[918]

8.13 The Commonwealth Privacy Act Review

8.13.1 The Commonwealth Privacy Act Review considered the effectiveness and operation of mandatory data breach notifications. This included inquiring into whether data security practices and awareness have changed since their introduction, and whether there have been challenges for entities that are required to comply with notification requirements in other jurisdictions (for example, the GDPR) on top of the Privacy Act obligations.[919] The Review reported that submitters 'indicated that the NDB scheme has raised awareness about the importance of effective data security and changed entities' data security practices' in a manner that did not impose an undue burden on regulated entities.[920]

8.13.2 In response to submissions expressing concern about a potential lack of alignment between the Commonwealth notification scheme and future schemes in other Australian jurisdictions, the Review recommended that further work be undertaken to facilitate reporting processes for notifiable data breaches for regulators and regulated entities.[921] The Government agreed with this proposal.[922]

8.13.3 The Review also recommended amendments to the scheme to:

---

[913] GDPR art 33.
[914] GDPR art 34.
[915] OAIC, *Notifiable Data Breaches Scheme 12-month Insights Report* (Report, 13 May 2019) 8.
[916] OAIC, *Notifiable Data Breaches Report January to June 2023* (Report, 5 September 2023) 5, 19, 29.
[917] *Privacy and Personal Information Protection Amendment Act 2022* (NSW) s 2; NSW Government, Statement of Public Interest, Privacy and Personal Information Protection Amendment Bill 2022 (NSW) 2 <https://www.parliament.nsw.gov.au/bill/files/4040/SPI%20-%20Privacy%20and%20Personal%20Information%20Protection%20Amendment%20Bill%202022.pdf>.
[918] See also Queensland Government, *Consultation Paper: Proposed Changes to Queensland's Information Privacy and Right to Information Framework* (June 2022) <https://www.publications.qld.gov.au/ckan-publications-attachments-prod/resources/7326cb08-a3da-451c-8c48-dc08ea9dcc6d/consultation-paper-proposed-changes-qld-ip-rti-framework.pdf?ETag=f9671bcc9b57d55cc316d1c803234761>.
[919] Privacy Act Review Report 2022 ch 28.
[920] Ibid 289.
[921] Privacy Act Review Report 2022 Proposal 28.1 and 290–291.
[922] Government Response 10.

- require notification to the Commissioner to take place within 72 hours after the entity becomes aware that there are reasonable grounds to believe that there has been an eligible data breach, with allowance for further information to be provided if it is not available within that time period;[923] this was characterised as being in line with 'community expectation… that individuals will be notified quickly if their personal information has been compromised';[924]
- require notification of individuals as soon as practicable and, where it is not possible to provide all information at the same time, to provide the information in phases as soon as practicable;[925] and
- oblige entities to 'take reasonable steps to implement practices, procedures and systems' to enable them to respond to a data breach quickly.[926]

8.13.4 The Government agreed in-principle with these proposals.

8.13.5 Also in response to perceived community expectations, the Review recommended that a requirement be placed on entities to state the steps they have taken or intend to take in response to a breach 'including, where appropriate, steps to reduce any adverse impacts on the individuals to whom the relevant information relates'.[927] The Review recommended that further consideration be given to whether entities should be required to take reasonable steps to prevent or reduce harm likely to arise for individuals, on the basis that this would complement the existing obligation on entities to notify individuals so they can take action to protect themselves.[928]

8.13.6 Finally, the Review proposed the introduction of a provision enabling the Attorney-General to permit the sharing of personal information with appropriate entities (for limited purposes and durations), where doing so would reduce the risk of harm from an eligible data breach. This would mirror changes made to the *Telecommunications Regulations 2021* in late-2022 to improve responses to large-scale telecommunications company data breaches by permitting the companies to share information with financial services entities, so they could apply enhanced monitoring and safeguards for customers whose information had been compromised.[929]

8.14 Consultation

8.14.1 The TLRI Issues Paper sought stakeholders' views on data breach notification requirements as follows:

> Should a form of data breach notification requirement be introduced? If so, what models of mandatory reporting schemes should be considered?[930]

8.14.2 Several submissions, including those of Meg Webb MLC, Dr Joel Scanlan, Richard Griggs, and Youth Law Australia, expressed support for the introduction of a data breach notification requirement in the PIPA.

[923] Privacy Act Review Report 2022 Proposal 28.2.
[924] Ibid 294.
[925] Ibid Proposal 28.2.
[926] Ibid.
[927] Ibid Proposal 28.3.
[928] Ibid Proposal 28.3 and 297.
[929] Ibid Proposal 28.4 and 297–298.
[930] Issues Paper Part 2, Question 2.15.

8.14.3 Youth Law Australia and Meg Webb MLC each submitted that recent data breaches in Tasmania (such as the announcement by the Tasmanian Department of Education, Children and Young People of a possible theft of data in March 2023)[931] highlighted the importance of data breach notification laws and public expectations that affected individuals will be notified by authorities respectively. Richard Griggs made a similar point that the damage that can be caused by data breaches is now understood, and expressed his expectation that data breach notification requirements would be consistent with public sentiment and good privacy practice.

8.14.4 Richard Griggs submitted that PIPP 4(2) (also discussed at [6.5.4] above) should be expanded to require notification of data breaches; that is, notification of individuals where there is misuse, loss, unauthorised access, modification, or disclosure of personal information. Mr Griggs suggested that such mandatory disclosure should 'contain practical and useful information that can be understood and acted upon by the individual'.[932]

8.14.5 Meg Webb MLC proposed an additional notification requirement that would apply where an entity has reasonable grounds to suspect there has been a data breach, whereby the entity must ascertain whether there are reasonable grounds to consider the breach did occur.

8.14.6 Dr Joel Scanlan submitted that simplicity is important in regulation, suggesting that a 28- or 30-day requirement to notify authorities of a breach, and principles such as the APPs, are fairly understandable to regulated entities.[933]

8.14.7 Dr Scanlan also noted advantages of schemes that enable regulators to issue or seek fines for a data breach, suggesting that a 'hammer' communicates to custodians that they are taking on a liability if they do not actually need information that they are collecting or otherwise handling. Dr Scanlan also noted that, in other jurisdictions, disclosure under notification schemes enables custodians to avoid fines.[934]

8.14.8 Dr Scanlan noted the importance of aligning data breach notification regulations across jurisdictions (including international jurisdictions), observing that Australian and Tasmanian bodies may be fined under the GDPR in relation to the data of European Union citizens.

8.15 The TLRI position

8.15.1 The TLRI is of the view that data breach notification schemes are an important tool for improving transparency and protection from privacy-related harm for individuals, as well as improving accountability and practices among regulated bodies and enhancing consistency across jurisdictions within Australia and internationally. Additional resources would need to be made available to enable personal information custodians to comply with data breach notification requirements.

[931] Clancy Balen and Meg Whitfield, 'Minister Confirms 16,000 Documents Released Online in Tasmanian Data Breach, Helpline Set Up' (*ABC News Online*, 7 April 2023) <https://www.abc.net.au/news/2023-04-07/tasmania-goanywheremft-file-share-data-breach-16k-documents-out/102197658>.
[932] Submission 10 (Richard Griggs).
[933] Submission 20 (Dr Joel Scanlan).
[934] Ibid.

8.16 Recommendations

Recommendation 55: The TLRI recommends that Tasmania introduce a data breach notification scheme based on the Commonwealth model.

Part 9

Other Legislation Impacting the Privacy of Government-held Information

9.1 Overview of this Part

9.1.1 In the TLRI Issues Paper, consideration was given to other legislative provisions outside the P*ersonal Information Protection Act 2004* (Tas) ('PIPA') that impact the privacy of government-held information. The issues paper raised three areas of focus which are further discussed in this Part:

- situations where legislation may override the privacy protections in the PIPA;[935]
- situations where legislation may impose secrecy obligations that can serve as privacy protections;[936] and
- situations where legislation provides for the gathering of personal information *without* specifically setting limits on its use or sharing, focusing on the context of sharing information within and between government agencies.[937]

9.2 Legislation which may override the PIPA

The Tasmanian position

9.2.1 Section 4 of the PIPA holds that provisions of the PIPA can be overridden by any inconsistent provisions in any other legislation.[938] This means that, where other legislation authorises the collection, use, or disclosure of personal information in a manner that would breach the PIPA, its requirements will not apply. However, it may not always be clear whether other legislation is inconsistent such as to override the PIPA. For example, legislation may authorise the collection of certain types of information without specifying how it can be collected or used. Alternatively, legislation may provide for restrictions which differ slightly from those in the PIPA.

9.2.2 For example, the Right to Information Act 2009 (Tas) provides a legally enforceable right for a person to be provided with information possessed by a public authority or a Minister.[939] The Act creates various exemptions that allow information to be withheld, where the public authority's principal officer or the Minister considers the disclosure to be contrary to the public interest.[940] For example, information can be withheld if disclosure would include a third party's personal information or

[935] See Issues Paper [3.2].
[936] See ibid [3.3].
[937] See ibid.
[938] PIPA s 4.
[939] *Right to Information Act 2009* (Tas) s 7. The Tasmanian Ombudsman has determined that the PIPA does not prevent the release of personal information under the *Right to Information Act 2009* (Tas): *Clive Stott and Hydro Tasmania* [2021] Ombudsman Tasmania, Decision 1702–115 [69].
[940] *Right to Information Act 2009* (Tas) ss 33.

information related to the business affairs of a third party.[941] While the public interest could nevertheless weigh in favour of disclosure, the principal officer or Minister must first consult the third party; the third party may apply for review of any decision to disclose their information. The legislation sets out 25 'matters to be considered when assessing if disclosure of particular information would be contrary to the public interest', which cover considerations such as accessibility and understanding of government decisions, public health or safety, the administration of justice, equity and fair treatment, and security and good order.[942] This list does not explicitly identify personal privacy as a matter to be taken into account in the application of the public interest test.

9.2.3 It is unclear whether the terms of the *Right to Information Act 2009* (TAS) ('RTI Act') is 'inconsistent' with the PIPA in the sense contemplated in Section 4 of the PIPA. Specifically, it is not clear whether the exemption from RTI Act disclosure requirements, where it is contrary to the 'public interest', would limit disclosure to the various circumstances where disclosure is also permitted under the Personal Information Protection Principles ('PIPPs'). In other words, it is unclear whether disclosure that would breach the PIPPs would be deemed *against* the public interest under the RTA Act, or whether there are circumstances in which disclosure that would not be permitted under the PIPA is permitted under the RTI Act—in which case, the RTI Act would prevail.

9.2.4 A clearer and direct example of inconsistency is found in legislation relating to Stolen Generation investigations. *The Stolen Generations of Aboriginal Children Act 2006* (Tas) expressly provides that the Stolen Generations Assessor (responsible for assessing information relevant to the investigations) is empowered to exercise their powers, notwithstanding legislative protections of confidentiality or privacy.[943] Another example is the information sharing framework created in Part 5 of the *Child and Youth Safe Organisations Act 2023* (Tas).[944] This allows for the sharing of personal information as permitted under the Act, and specifically states that the PIPA does not apply in certain circumstances connected with the obtaining or possession of information or to information obtained or possessed for the purposes of the *Child and Youth Safe Organisations Act 2023* (Tas).[945] The *Commissions of Inquiry Act 1995* (Tas) also provides that the PIPA does not apply to any information collected for communication to, or communicated to, the Commission of Inquiry into Institutional Child Sexual Abuse'.[946]

9.2.5 A number of other Acts address the application of the PIPA in various ways. For example, some provide that the Act overrides PIPA, while others hold that the provisions of the Act have effect despite PIPA or to the extent of any inconsistency.

- The *Family Violence Act 2004* (Tas) provides that a personal information custodian acting in good faith does not commit a breach of the PIPA 'by reason only of collecting, using, disclosing or otherwise dealing with personal information for the purpose of furthering the objects of [the *Family Violence Act 2004*]'.[947]

[941] *Right to Information Act 2009* (Tas) ss 36, 37. See ss 38–39 for other exemptions subject to a public interest test, including disclosure of information relating to a public authority's business affairs and information obtained in confidence.
[942] See *Right to Information Act 2009* (Tas) sch 1.
[943] *Stolen Generations of Aboriginal Children Act 2006* (Tas) s 16(2).
[944] *Child and Youth Safe Organisations Act 2023* (Tas) ss 38, 39, 40.
[945] *Child and Youth Safe Organisations Act 2023* (Tas) s 39(3).
[946] *Commissions of Inquiry Act 1995* (Tas) s 7A.
[947] *Family Violence Act 2004* (Tas) s 37.

- The *Children, Young Persons and Their Families Act 1997* (Tas) provides that the PIPA applies to 'information received and provided under this Act to the extent that it is not inconsistent with the provisions of the Act'.[948]
- The *Corrections Act 1997* (Tas) relates to disclosure of critical health information by health officials and provides that the relevant subsection 'has effect despite the [PIPA] or other law relating to confidentiality or privacy of information'.[949]
- The *Dangerous Criminals and High Risk Offenders Act 2021* (Tas), which provides that a person who is a personal information custodian within the meaning of the [PIPA] is not taken to contravene that Act by reason only of collecting, using, disclosing, or otherwise dealing with, personal information, for the purposes of [the *Dangerous Criminals and High Risk Offenders Act 2021*].[950]
- The *End-of-Life Choices (Voluntary Assisted Dying) Act 2021* (Tas) provides that the Commission may require evidence to be lodged and that this provision applies, despite the PIPA and any rule of law relating to privilege or the public interest in relation to the production of documents.[951]
- The *Sentencing Act 1997* (Tas) provides that, in relation to drug treatment orders, a 'person who is a personal information custodian within the meaning of the [PIPA] is not taken to contravene that Act by reason only of collecting, using or disclosing or otherwise dealing with personal information for the purposes of this Part'.[952]
- The *Youth Justice Act 1997* (Tas) provides for protection against prosecution in relation to certain disclosures of information and that the provision has effect 'despite the [PIPA] or any other law relating to the confidentiality or privacy of information'.[953]
- The *Registration to Work with Vulnerable People Act 2013* (Tas) provides that the '[PIPA] does not apply to the obtaining or possession of information by an official for the purposes of this Act'.[954]

9.2.6 As noted, some legislation does not specifically refer to the PIPA but may contain provisions that are inconsistent with it. For example, Part VI of the *Adoption Act 1988* (Tas) allows for access to information under the Act, and protects privacy other than where information can be disclosed under the Part. However, it does not specifically refer to the PIPA.[955]

9.2.7 In contrast, the *Education Act 2016* (Tas) provides that obligations to provide information are subject to the obligations under the PIPA.[956] Information sharing by the Teachers Registration Board is permitted under the provisions of the *Teachers Registration Act 2000* (Tas), which sets out the

[948] *Children, Young Persons and Their Families Act 1997* (Tas) s 111B.
[949] *Corrections Act 1997* (Tas) s 87C.
[950] *Dangerous Criminals and High Risk Offenders Act 2021* (Tas) s 46. See also s 47, which provides for the disclosure of compliance information, and ss (3), which provides that the requirement to comply with a request for information from a judge, magistrate, or relevant officer 'has effect despite the [PIPA] or other law relating to confidentiality of privacy of information'.
[951] *End-of-Life Choices (Voluntary Assisted Dying) Act 2021* (Tas) s 101.
[952] *Sentencing Act 1997* (Tas) s 27U.
[953] *Youth Justice Act 1997* (Tas) s 167A.
[954] *Registration to Work with Vulnerable People Act 2013* (Tas) s 57.
[955] The *Adoption Act 1988* (Tas), s 75 creates a protection for privacy in so far as 'a person shall not, under this Part, give to an applicant under this Part, and an applicant under this Part is not entitled to obtain, information relating to the personal affairs of a person, whether living or dead, other than the applicant or from which another person may be identified, whether directly or indirectly, except subject to and in accordance with this Part'.
[956] *Education Act 2016* (Tas) ss 42(10), 62.

circumstances in which the Board can share information.[957] In exercising its functions, the Final Report of the Commission of Inquiry into the Tasmanian Government's Responses to Child Sexual Abuse in Institutional Settings ('CoI') set out the difficulties that the Board had experienced in receiving information from other agencies about teachers regulated by the Board. It was noted that legal advice based on the interpretation of the PIPA meant that the Department of Education's view was that it could not disclose information collected in its investigation to a third party.[958] To address this, the CoI made recommendations to better facilitate information sharing and the disclosure of information.[959]

The position in other jurisdictions

9.2.8 In other jurisdictions, although approaches differ, there is generally greater legislative clarity about the relationship between privacy constraints and legislation providing for freedom of information (and the operation of the public interest test) than is provided in the equivalent Tasmanian legislation. There is also specific legislative direction as to how matters of privacy are to be taken into account when applying the public interest test.

9.2.9 For example, in Victoria, the *Privacy and Data Protection Act 2014* (Vic) provides that nothing in that Act affects the operation of the *Freedom of Information Act 1982* (Vic) or any right, privilege, obligation, or liability conferred or imposed under that Act or any exemption arising under that Act.[960] The *Freedom of Information Act 1982* (Vic) provides that personal affairs information is exempt from disclosure, where disclosure would be unreasonable in the circumstances.[961] As with Victoria, under the *Freedom of Information Act 1982* (Cth), personal information is conditionally exempt from disclosure, if it would involve the unreasonable disclosure of personal information.[962]

9.2.10 As in Victoria, New South Wales legislation makes it clear that the *Privacy and Personal Information Protection Act 1998* (NSW) does not affect the operation of or lessen any obligations of a public sector agency under the *Government Information (Public Access) Act 2009* (NSW).[963] There is also a provision that establishes the relevance of privacy considerations arising under the *Privacy and Personal Information Protection Act 1998* (NSW) to the public interest test for disclosure under *Government Information (Public Access) Act 2009* (NSW).[964] Similarly, in Queensland, the *Right to Information Act 2009* (Qld) states that the Act 'overrides the provisions of other Acts prohibiting the

[957] See discussion in CoI Report 184.
[958] Ibid 185.
[959] Ibid Recommendation 6.10.
[960] *Freedom of Information Act 1982* (Vic) s 6(2). See also s 14, which contains an explicit exemption for the Act from the application of IPP 6.
[961] *Freedom of Information Act 1982* (Vic) s 33. See OVIC, *Section 33 – Document affecting Personal Privacy* (Web Page, 2024) <https://ovic.vic.gov.au/freedom-of-information/foi-guidelines/section-33/>.
[962] *Freedom of Information Act 1982* (Cth) s 47F. See OAIC, *Freedom of Information Guidelines* <https://www.oaic.gov.au/freedom-of-information/freedom-of-information-guidance-for-government-agencies/foi-guidelines/part-6-conditional-exemptions#documents-affecting-personal-privacy-s-47f>.
[963] *Privacy and Personal Information Protection Act 1998* (NSW) s 5.
[964] *Government Information (Public Access) Act 2009* (NSW) s 14; Table 3(b).

disclosure of information (however described)'.[965] It also specifies that the right to privacy of an individual is a factor favouring non-disclosure in the public interest test.[966]

9.3 The Commonwealth Privacy Act Review

9.3.1 As part of the Commonwealth Privacy Act Review, feedback was sought on proposals to deal with interactions between the *Privacy Act 1988* (Cth) and other privacy legislation or schemes that contain privacy protections.[967] In response, it was proposed that the Attorney-General's Department develop a 'privacy law design guide' to support Commonwealth agencies when developing new schemes with privacy-related obligations. This was seen to be a 'good first step to providing a more structured framework for considering the privacy legislation landscape' and that '[o]nce developed, it would be open for there to be further consideration about whether there would be benefit in reviewing existing legislative schemes to achieve greater harmonisation'.[968] The Government agreed in-principle with this proposal.[969]

9.4 Consultation

9.4.1 The TLRI Issues Paper did not ask any questions relating to legislation that may override the PIPA or, more specifically, about the scope of the public interest exception under the RTI Act. However, some submissions identified issues concerning the relationship between the PIPA and the RTI Act that make the interpretation and application of provisions problematic.[970]

9.4.2 The Commissioner for Children and Young People also noted that privacy considerations (and the PIPA) are relevant to the *Children Young Persons and their Families Act 1997* (Tas) and the *Youth Justice Act 1997* (Tas), and that there was a need to balance the right to privacy with the right to be safe in setting limits on information sharing. Information sharing was also raised in the Tasmania Legal Aid submission. This issue is discussed at [9.10] below.

9.4.3 The Commissioner for Children and Young People observed that the Issues Paper for this project did not examine in detail the *Children Young Persons and their Families Act 1997* (Tas), the *Youth Justice Act 1997* (Tas), or other legislation that raises privacy issues in relation to children and submitted that children's privacy must be considered in future reviews of those Acts.

[965] *Right to Information Act 2009* (Qld) s 6. The Act also sets out details about the relationship between the *Information Privacy Act 2009* (Qld) in s 8. This is amended by the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) (yet to be commenced). There is also a provision setting out the relationship with the *Right to Information Act 2009* (Qld) in the *Information Privacy Act 2009* (Qld) s 9. This is omitted by the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) (yet to be commenced).
[966] *Right to Information Act 2009* (Qld) s 49, sch 4, Pt 3. See also sch 4, pt 4, cl 6, which sets our factors favouring non-disclosure in the public interest because of public interest harm in disclosure. It is noted that the *Information Privacy and Other Legislation Amendment Act 2023* (Qld) (yet to be commenced) amends s 49 and Schedule 4 in relation to the public interest test.
[967] Privacy Act Review Report 2022: see discussion at 29.1.
[968] Ibid 29.1.1.
[969] Government Response 37.
[970] See discussion at [6.5.6] and following.

9.4.4 The relationship between the *Family Violence Act 2004* (Tas) and the PIPA was also raised in one submission.[971]

9.4.5 Other feedback received highlighted a lack of clarity in relation to where the PIPA sits in the hierarchy of legislation and that there is a possibility that the number of other pieces of legislation which exempt themselves from the PIPA is too broad.[972] It was also noted that the 2021 Independent Review of the State Service recommended that 'the government develop and fund a stronger whole-of-government capacity for sharing, linking and analysing data'.[973]

9.5 The TLRI's view

9.5.1 As has been recognised, rights relating to the handling of personal information and right to information held by government are closely related.[974] However, unlike other jurisdictions, in Tasmania there is a lack of clarity as to relationship between the privacy protections in the PIPA and freedom of information rights in the RTI Act.

9.5.2 There is also uncertainty regarding the interaction of the PIPA with other legislative schemes that have provisions restricting the sharing of government-held information or provide for access to information. For example, it is difficult for custodians of information to know how other legislation interacts with or overrides the PIPA.

9.5.3 The TLRI also notes the comments made by the Commissioner for Children and Young People in relation to information sharing about sharing in the context of child protection under the *Children, Young Persons and their Families Act 1997* (Tas) and of youth justice under the *Youth Justice Act 1997* (Tas). As part of the recently released, *Youth Justice Blueprint*, Strategy 4 was to integrate and connect whole-of-government and community service systems though active communication between agencies and the sharing of information.[975] In doing so, the Blueprint adopts the CoI's proposal that the privacy and secrecy provisions in legislation such as the *Children, Young Persons and Their Families Act 1997* (Tas) and the PIPA should be reviewed to assist agencies and statutory bodies to work effectively with one another and share information.[976]

9.5.4 The TLRI notes the extensive consultation process undertaken by the CoI and its conclusion that there is a need for greater clarity in the relationship between the RTI Act and the PIPA (discussed further at [6.6.13] and following), as well as the need to identify and respond to legislative barriers to information sharing relating to child safety, and to address cultural barriers that exist in Tasmanian government departments.[977]

9.5.5 Accordingly, it is the TLRI's view that there should be a close examination of the relationship between the provisions of the PIPA and other Tasmanian legislation with a view to obtaining greater

[971] Submission 22 (Anonymous).
[972] Submission 10 (Richard Griggs).
[973] Ian Watt, *Independent Review of the Tasmanian State Service: Final Report* (2021), Recommendation 19 <https://www.dpac.tas.gov.au/__data/assets/pdf_file/0026/136934/TSSR_Final_Report.pdf>
[974] See also Department of Justice and Attorney-General (Qld), *Proposed Changes to Queensland's Information Privacy and Right to Information Framework* (Consultation Paper, 2022) 10.
[975] Department for Education, Children and Young People, *Youth Justice Blueprint 2024 – 2034: Keeping Children and Young People Out of the Youth Justice System* (2023) 33 <https://publicdocumentcentre.education.tas.gov.au/library/Shared%20Documents/Youth-Justice-Blueprint.pdf>.
[976] CoI Final Report 75 and Recommendation 19.7.
[977] Ibid 42–43.

harmonisation and consistency between them. A model to consider in such a review may be to develop a privacy law design guide as a starting point for evaluation, in line with the proposal of the Privacy Act Review.

9.6 Recommendation

Recommendation 56: There should be a close examination of the relationship between the provisions of the PIPA and other Tasmanian legislation with a view to obtaining greater harmonisation and consistency between them. In this review, there is a need to ensure privacy protection is maximised to the extent that is possible in balance with other policy interests

9.7 Legislation that restricts the sharing of government-held information

9.7.1 The TLRI Issues Paper observed that, while certain legislation may override privacy protections in the PIPA, legislation can also provide for secrecy of information in a way that may protect private information from various forms of disclosure. Typically, these provisions apply to government officials or agents whose roles involve collecting or using private information. They prevent these officials or agents from using or disclosing information in an unauthorised way and unauthorised disclosure may be subject to penalties.[978]

9.7.2 For example, there are secrecy obligations on:

- law enforcement officers in the context of financial reporting;[979]
- individuals administering the First Home Owner Grant scheme;[980]
- individuals dealing with occupational licensing;[981]
- officers dealing with the registration of those authorised to work with vulnerable people;[982]
- individuals involved in the governance of the Australian Crime Commission,[983] Corporate Affairs,[984] and Consumer Affairs;,[985] and
- individuals involved in processing workers' rehabilitation and compensation claims.[986]

9.7.3 However, these provisions are not necessarily a guarantee against disclosure in all circumstances. First, the provisions vary in the degree of privacy protection they afford. Second, as

[978] See, eg, *First Home Owner Grant Act 2000* (Tas) s 40(3).
[979] *Financial Transaction Reports Act 1993* (Tas) s 10.
[980] *First Home Owner Grant Act 2000* (Tas) s 40.
[981] *Occupational Licensing Act 2005* (Tas) s 51.
[982] *Registration to Work with Vulnerable People Act 2013* (Tas) s 54.
[983] *Australian Crime Commission Act 2004* (Tas) s 44.
[984] *Commissioner for Corporate Affairs Act 1980* (Tas) s 6E.
[985] *Consumer Affairs Act 1988* (Tas) s 22.
[986] *Workers Rehabilitation and Compensation Act 1988* (Tas) s 158.

found under the PIPA, there are exceptions for when information can nevertheless be disclosed.[987] While a variety of approaches are taken, typical exceptions include where the disclosure is:

- in relation to the enforcement of laws of the State, Commonwealth, or another State or Territory;[988]
- in relation to carrying out functions under or in administration of the legislation in question;[989]
- considered necessary or appropriate in the public interest generally;[990]
- related to legal proceedings;[991]
- related to research or statistical analysis purposes;[992] or
- only to specified agencies or officers, who may, but may not, be subject to restrictions on the handling of the information in question.[993]

9.7.4 In some cases, these restrictions may be considered in terms of their proportionality to their potential impacts on privacy. However, there is a lack of consistency in approach. The restrictions may also be drafted in general terms, which can cause uncertainty over the extent to which they are inconsistent with the PIPA obligations or the extent to which privacy considerations must be taken into account in decisions to share information.

9.7.5 There are also restrictions on the disclosure of information contained in Section 194K of the *Evidence Act 2001* (Tas) in relation to the publication of identifying information about a person in respect of whom specific crimes involving a sexual offence are alleged to have been committed and also any witness or intended witness to those proceedings.[994] Difficulties caused by this provision were raised in the context of the CoI. A reference examining the issue from the Tasmanian Attorney-General was accepted by the TLRI in November 2023.[995]

9.8 Consultation

9.8.1 The TLRI Issues Paper did not ask any questions relating to legislation that may restrict the sharing of government-held information and potential inconsistencies with the PIPA. no submissions specifically addressed this issue.

---

[987] See, eg, *First Home Owner Grant Act 2000* (Tas) s 40; *First Home Owner Grant Regulations 2021* (Tas) s 6. Examples of exceptions for when information can be disclosed include: where the person to whom the information relates requests or consents to disclosure; where it is for the purposes of legal proceedings; or where disclosure is in connection with the administration or enforcement of tax law.

[988] *Financial Transaction Reports Act 1993* (Tas) s 10*; First Home Owner Grant Act 2000* (Tas) s 40; *Occupational Licensing Act 2005* (Tas) s 51; *Home Builder Grants Act 2020* (Tas) s 52; *Asbestos-Related Diseases (Occupational Exposure) Compensation Act 2011* (Tas) s 184.

[989] *Consumer Affairs Act 1988* (Tas) s 22; *Registration to Work with Vulnerable People Act 2013* (Tas) s 54; *Valuation of Law Act 2001* (Tas) s 58; *Tasmanian Development Act 1983* (Tas) s 45; *Industrial Relations Act 1984* (Tas) s 83; *Health Practitioners Tribunal Act 2010* (Tas) s 54.

[990] *Gaming Control Act 1993* (Tas) s 157; *Vehicle and Traffic (Driver Licensing and Vehicle Registration) Regulations 2010* (Tas) s 125.

[991] *Threatened Species Protection Act 1995* (Tas) s 59.

[992] *Asbestos-Related Diseases (Occupational Exposure) Compensation Act 2011* (Tas) s 184.

[993] *First Home Owner Grant Regulations 2010* (Cth) s 6.

[994] It is also noted that the *Youth Justice Act 1997* (Tas) s 31 also contains a prohibition on anyone publishing information identifying, or which may lead to the identification of, a youth the subject of, or a witness in, proceedings.

[995] CoI Final Report 321–323.

9.9 The TLRI's view

9.9.1 As the Issues Paper identified, there is uncertainty regarding the interaction of the PIPA with other legislative schemes which have provisions restricting the sharing of government-held information. The TLRI's view is that greater harmonisation in this area could form as part of the project examining the relationship between the PIPA and provisions in other Tasmanian legislation recommended above.[996]

9.10 Legislation that facilitates the sharing of information within and between government agencies

9.10.1 The nature of government means that its operations are structured into various departments and agencies. Provision for information sharing within and between government agencies has been identified as vital to good government. For instance, information is an asset that is essential for developing informed policy, and data exchange across agencies provides for better government-wide statistical capability.[997] It also can also be for the public benefit.[998] This has been identified as an issue in the Tasmanian context in the CoI.[999] The need for a review of the legislative framework around sharing information across agencies for the purpose of protecting the safety and wellbeing of children and young people was identified, and such a review recommended, by the CoI.[1000]

9.10.2 Information sharing within and between government departments can be facilitated by legislation. If the legislative provisions provide for the gathering of personal information *without* specifically providing for limitations on its use or sharing, this may jeopardise information privacy.

The Tasmanian position

9.10.3 The PIPA provisions enabling sharing of 'basic personal information'[1001] with public authorities represents a potential gap in protection under the PIPA. As discussed above at [4.12.4], the PIPA allows personal information custodians to share this type of information with other public authorities where the use or disclosure is reasonably necessary for the efficient storage and use of that information, regardless of whether this accords with the purpose for which the information was collected or whether the person has consented.[1002] There may therefore be scope for Tasmanian government agencies to share certain information without being restricted by obligations under the PIPA or by other privacy considerations.

9.10.4 As noted above at [9.2.5], legislative frameworks that permit sharing of personal information are also found in other legislation. For example, a framework for sharing personal information within government agencies and outside government was created by the Child and Youth Safe Organisations Act 2023 (Tas). Sharing of information is also addressed in other Acts, including the *Family Violence*

[996] See Recommendation 30 at [5.7].
[997] See discussion in OVIC, *Information Sharing and Privacy: Guidance for Sharing Personal Information (2021)* 5–6; Information and Privacy Commission New South Wales, *Data Sharing and Privacy: A Guide for Public Sector Agencies* (2020) 3 <https://www.ipc.nsw.gov.au/sites/default/files/2021-03/Guide_Data_Sharing_and_Privacy_July_2020.pdf>.
[998] Ibid.
[999] See [9.10].
[1000] CoI Report Recommendation 19.7.
[1001] The name, residential address, postal address, date of birth, and gender of an individual: PIPA s 3 (definition of 'basic information').
[1002] PIPA s 12.

Act 2004 (Tas),[1003] *Commissioner for Children and Young People Act 2016* (Tas),[1004] *Dangerous Criminals and High Risk Offenders Act 2021* (Tas),[1005] *Disability Services Act 2011* (Tas),[1006] *Education Act 2016* (Tas),[1007] *Sentencing Act 1997* (Tas),[1008] *Work Health and Safety Act 2012* (Tas),[1009] and the *Youth Justice Act 1997* (Tas).[1010]

9.10.5 The sharing of information across government agencies in Tasmania is managed by the Administrative Data Exchange Protocol for Tasmania ('ADEPT'), which is intended to be read in conjunction with the obligations under the PIPA. ADEPT is a set of guidelines 'developed in response to the need for a shared understanding of privacy responsibilities and practical guidelines for the collaborate exchange and integration of data within and across Tasmanian Government agencies'.[1011] The protocol aims to 'promote and manage cross-Agency information exchange in ways that are open, transparent and secure'.[1012] ADEPT includes a set of principles and procedures intended to ensure that proper safeguards are in place when exchanging data within and between agencies in the public interest.[1013] One principle is safe authorisation, which mandates that provisos of data privacy, confidentiality, security, and intellectual property are respected and protected. This is especially crucial, given that, as ADEPT recognises, much of 'data considered essential for population-based research and policy decisions contains personal and often sensitive information'.[1014]

9.10.6 As part of the principle of safe authorisation, agencies must follow ADEPT procedures to ensure that data use and disclosure complies with PIPP 2(1)(c) when exchanging data for use in research or statistical analysis. This allows a custodian to use or disclose information for research or statistical analysis purposes (even if this was not the initial purpose for collection), provided it does not identify an individual and either: (1) it is impracticable to seek the individual's consent; or (2) the custodian reasonably believes that the recipient is not likely to disclose the information.[1015] In relation to the exchange of data which involves personal or sensitive information about individuals, the procedures for releasing data require evaluation based on the PIPA, including Principles 2 and 4 and against levels of security and standards appropriate to the privacy impact and risk assessment.[1016]

9.10.7 While privacy is a significant value in information management, it is not always the overriding interest. In the context of information sharing, the relationship between privacy and safety has been identified by the CoI.[1017] The CoI recommended that the government review confidentiality and privacy provisions in legislation such as the *Children, Young Persons and their Families Act 1997* (Tas), *Registration to Work with Vulnerable People Act 2013* (Tas), and the PIPA 'to identify legislative barriers to sharing information across agencies for the purpose of protecting the safety and wellbeing

[1003] *Family Violence Act 2004* (Tas) s 53B.
[1004] *Commissioner for Children and Young People Act 2016* (Tas) Pt 2 Div 3.
[1005] *Dangerous Criminal and High Risk Offenders Act 2021* (Tas) s 46.
[1006] *Disability Services Act 2011* (Tas) s 50.
[1007] *Education Act 2015* (Tas) ss 224B and 231F.
[1008] *Sentencing Act 1997* (Tas) s 27U.
[1009] *Work Health and Safety Act 2012* (Tas) sch 2, pt 2, cl 4.
[1010] *Youth Justice Act 1997* (Tas) ss 22(4A), 31, 45 and 167A.
[1011] Department of Premier and Cabinet, *Digital Data Privacy* (Web Page) <https://www.dpac.tas.gov.au/divisions/digital_strategy_and_services/policies/digital_data_privacy>.
[1012] Department of Premier and Cabinet, *ADEPT Principles* (Web Page) <http://www.dpac.tas.gov.au/divisions/digital_strategy_and_services/policies/digital_data_privacy/adept>.
[1013] Ibid.
[1014] Ibid.
[1015] Department of Premier and Cabinet, *ADEPT Principles*. For more discussion in relation to the research exemption, see [9.11.2].
[1016] Ibid.
[1017] This is discussed further in relation to information sharing within government: see [9.13.3].

of children and young people'.[1018] The CoI considered that such barriers as were identified should be removed but considered that the primary barrier to information sharing was a 'deeply held view across many parts of the Government that prioritises privacy over child safety'.[1019]

The position in other jurisdictions

9.10.8 As noted at [4.12.21], the Commonwealth *Privacy Act 1988* (Cth) ('Privacy Act') and other State and Territory privacy legislation does not specify different rules for the handling of personal information that is basic information.

9.10.9 Other jurisdictions have taken measures to provide a legislative basis for the sharing of government-held information within and between agencies (and in some cases beyond government) in a way that explicitly seeks to preserve privacy protections.

9.10.10 In NSW, the *Data Sharing (Government Sector) Act 2015* (NSW) provides authority for NSW government sector agencies to share information within government for limited purposes, including for efforts to improve government policy making, program management, as well as service planning and delivery.[1020] This Act provides that government sector agencies can share data for specific purposes and 'operates to authorise data sharing that might otherwise be prohibited under other legislation'.[1021] It is also possible to share data with private organisations. Agencies must comply with NSW privacy legislation[1022] and other privacy safeguards, including using contractual measures to restrict the use of information shared with non-government agencies and reporting potential privacy contraventions.[1023]

9.10.11 In Victoria, the *Victorian Data Sharing Act 2017* (Vic) creates a legislative framework for data sharing within government departments and agencies. The Act sets out the process for data sharing and contains requirements to notify of possible breaches, the continuation of privacy obligations, and creates offences for unauthorised access, use, or disclosure of information.[1024] It allows for sharing identifiable data (personal and health information) for the purposes of 'informing government policy making, service planning and design'.[1025] Identifiable data can be shared with the Chief Data Officer or a data analytics body for the purpose of data integration but other obligations under *Privacy and Data Protection Act 2014* (Vic) or the *Health Records Act 2001* (Vic) in relation to the handling of identifiable data are not affected.[1026]

9.10.12 At the Commonwealth level, the *Data Availability and Transparency Act 2022* (Cth) has been enacted, following recommendations of the Productivity Commission in its Data Availability and Use inquiry[1027] and the Office of the National Data Commissioner's *Best Practice Guide to Applying Data*

[1018] CoI Final Report 75.
[1019] Ibid.
[1020] *Data Sharing (Government Sector) Act 2015* (NSW) s 6.
[1021] Information Privacy Commission NSW, *Guide – Data Sharing and Privacy* <https://www.ipc.nsw.gov.au/guide-data-sharing-and-privacy>
[1022] *Privacy and Personal Information Protection Act 1998* (NSW); *Health Records and Information Privacy Act 2002* (NSW).
[1023] See *Data Sharing (Government Sector) Act 2015* (NSW) pt 3. See discussion in New South Wales, *Data Sharing and Privacy: A Guide for Public Sector Agencies* (2020) <https://www.ipc.nsw.gov.au/sites/default/files/2021-03/Guide_Data_Sharing_and_Privacy_July_2020.pdf>.
[1024] See *Victorian Data Sharing Act 2017 – Guidance for Departments and Agencies* <https://ovic.vic.gov.au/privacy/resources-for-organisations/information-sharing-and-privacy/>.
[1025] *Victorian Data Sharing Act 2017* (Vic) s 5.
[1026] *Victorian Data Sharing Act 2017* (Vic) ss 15, 24(2).
[1027] Productivity Commission, *Data Availability and Use Final Report* (Report, May 2017) <https://www.pc.gov.au/inquiries/completed/data-access/report>.

Sharing Principles in 2019.[1028] The Act is supported by the *Data Availability and Transparency Code* 2022. The scheme provides for sharing government data consistent with the *Privacy Act 1988* (Cth) for three purposes: (1) government service delivery; (2) informing government policies and programs; and (3) research and development. It sets out penalties for breaches of the regime.[1029] It creates an independent regulator (the National Data Commissioner) and provides authority for government agencies to share information between themselves, state and territory government agencies, and various other organisations (defined as 'accredited users'). In relation to privacy, agencies must seek the consent of any individuals before sharing personal information, unless it is unreasonable or impracticable to do so.[1030] The *Data Availability and Transparency Act 2022* (Cth) makes clear that data sharing must be consistent with the *Privacy Act 1988* (Cth).[1031] Any sharing must comply with data sharing principles which require the agency to consider:

- the appropriateness of the sharing, given the nature of the project;
- who the information will be shared with;
- the setting in which the information will be shared; and
- whether the information shared and the outputs from the project are limited to the minimum necessary to achieve the permitted purpose.[1032]

9.10.13 Another proposal at the Commonwealth level is the *Identity-matching Services Bill* 2019. This seeks to authorise the exchange of identity information between Commonwealth, state, and territory governments for use with identity-matching services, including facial recognition services.[1033] This has not been passed by Parliament as yet.

9.10.14 In contrast to NSW, Victorian and the Commonwealth position, in Queensland (as with Tasmania) the data sharing framework between government agencies is created by guidelines rather than legislation.[1034] The Queensland *Information Sharing Authorising Framework* is aimed at facilitating data sharing; the guidance makes it clear that '[a]lthough the privacy of individuals must be protected in accordance with the *Information Privacy Act 2009* (Qld) when sharing information, the existence of personal information should not in itself be a barrier to sharing'.[1035] The 'framework does not replace, negate or override legislative provisions that are in place to protect the privacy and confidentiality of citizens, but aims to better inform decisions that balance the risks associated with sharing activities and the business outcomes sought'.[1036]

[1028] Office of the National Data Commissioner (Department of Prime Minister and Cabinet), *Best Practice Guide to Applying Data Sharing Principles* (2019).
[1029] Office of the National Data Commissioner, *Office of the National Data Commissioner* <https://www.datacommissioner.gov.au/the-data-scheme>.
[1030] See the *Data Availability and Transparency Act 2022* (Cth) s 16B(4)(a); *Data Availability and Transparency Code 2022* (Cth) s 21.
[1031] *Data Availability and Transparency Act 2022* (Cth) s 17(5).
[1032] *Data Availability and Transparency Act 2022* (Cth) s 16.
[1033] *Identity–matching Services Bill 2019* (Cth).
[1034] See Queensland Government, *Information Sharing Authorising Framework* <https://www.forgov.qld.gov.au/information-and-communication-technology/qgea-policies-standards-and-guidelines/information-sharing-authorising-framework>.
[1035] Ibid 17.
[1036] Queensland Government, *Information Sharing Authorising Framework* 7.

9.11 The Commonwealth Privacy Act Review

9.11.1 The Commonwealth Privacy Act Review did not give consideration to the protection of basic personal information as an issue separate from the protection of personal information more generally.

9.11.2 Relevant to the operation of ADEPT in Tasmania, the Commonwealth Review considered the scope of the research exemption under the *Privacy Act 1988* (Cth) and noted that the *Data Availability and Transparency Act 2022* (Cth) scheme permits the sharing of public sector data containing personal information among government agencies (including states and territories) and with universities for research without consent, where Section 95 of the *Privacy Act* applies and other requirements are met.[1037]

9.12 Consultation

9.12.1 The TLRI Issues Paper invited submissions on the approach that should be taken to the sharing of information between government agencies in the following terms:

> Should legislation providing for the application of minimum privacy safeguards be introduced to apply to all information sharing within and between government bodies?[1038]
>
> If such legislation should be introduced, how should the safeguards be enforced?[1039]

9.12.2 Submissions were received about information sharing between government agencies, as well as between government and non-government agencies.

9.12.3 Some of the submissions concerning the sharing of information between government agencies focused on the risks of information sharing and suggested that it was necessary to ensure that information going between departments did not get into the wrong hands.[1040] Meg Webb MLC indicated that her view was that legislation should provide for the application of minimum privacy safeguards to apply to all information sharing within and between government bodies. Her view was that this must apply to all tiers of government (that is, local government, state government and federal government), including contractors and subcontractors. In terms of the enforcement of safeguards, Meg Webb MLC suggested that this could be potentially enforced via a stipulated regular independent auditor (such as an Office of the Australian Information Commissioner ('OAIC') and the Ombudsman), with the reports tabled in Parliament. It was suggested that further appeals to the courts and/or compensation may be applicable.[1041]

9.12.4 The Tasmanian Council of Social Service ('TasCOSS') recognised the need for there to be a balance between privacy and information exchange: 'it's important our approach to privacy allows for information exchange (including between agencies where appropriate) whilst ensuring the right to information and bodily privacy are promoted and respected'. Tasmania Police also stated that it

[1037] See Part 5.
[1038] Issues Paper Part 3, Question 3.1.
[1039] Ibid Part 3, Question 3.2.
[1040] Submission 3 (Anonymous).
[1041] See [8.4.12] in relation to the proposals to made changes to appeal options and the remedies that are available.

recognised and respected the right to personal privacy but pointed to the need for this to be balanced with public safety in allowing for the sharing of information.

9.12.5 In the submissions received by the TLRI, the need to balance privacy and safety was specifically identified in relation to children and young people.[1042] Youth Law Australia expressed the view that, while the right to privacy was an important right, it was 'not absolute, and it must be balanced with other rights'. This includes (as recognised by the Commonwealth Royal Commission into Institutional Responses to Child Sexual Abuse) 'rights to safety and wellbeing, and specifically to protection from sexual abuse [which] should be prioritised over other rights and concerns, including in some cases privacy'. Youth Law Australia pointed to the need for consistent and simplified privacy laws to facilitate the sharing of information. It noted that the Royal Commission into Institutional Responses to Child Sexual Abuse heard evidence that it can be difficult for institutions to navigate the privacy environment, and that this can inhibit sharing of information relating to the privacy and wellbeing of children. It was noted that, even where laws do not legally prevent sharing, concerns about privacy may have that effect.

9.12.6 In relation to information sharing, Youth Law Australia highlighted the importance of consultation of children and young people, where appropriate, before information about them is shared under information sharing schemes. The Commissioner for Children and Young People also identified the need to create a mechanism to involve children in decisions that affect their private information. In addition, the Commissioner stressed the need for privacy and children to be the subject of its own dedicated review, and to have the issues addressed in more detail than in the Issues Paper for the present project. The Commissioner highlighted the need to balance a child's right to privacy with the need to ensure that the care of the child is in their best interest in information sharing: 'How much do we share with people to ensure we uphold the child's right to privacy and their right to safety?'.

9.12.7 Tasmania Legal Aid ('TLA') recognised the need for both privacy and safety considerations to be taken into account in the context of family violence. TLA highlighted the importance of effective and consistent data recording and data sharing as a key to recognising behaviours which indicate risk of any violence, of escalation, of serious harm, and of lethality, to understand the prevalence and to assist in the reduction of harm. TLA observed that there are two major intersections of privacy and safety in the context of family violence:

- where information sharing is needed for a person and/or organisation to understand and adequately respond to risk of harm—encouraging broad and easy sharing of personal information; and
- where sharing information contributed to a risk of harm by: (1) family violence offenders and those supporting them (including systems and organisations) accessing information about the victim-survivors; or (2) disseminating information about the victim-survivor, such as images or mental health information; and (3) by victims-survivors experiencing negative consequences of information sharing or becoming reluctant to share information if it may be disclosed, or to access a service which may disclose information.

9.12.8 Issues that arise in relation to information sharing do not only apply to sharing between government agencies, as discussed by TLA: '[p]rivacy and safety considerations are significant to the question of how information-sharing about family violence can occur between government and non-government organisations'.

[1042] Submission 21 (Commissioner for Children and Young People); Submission 12 (Youth Law Australia); Submission 22 (Anonymous). Further discussion of the law in relation to privacy and young people is discussed at [10.4].

9.12.9 Other submissions focussed on the need for there to be provision for sharing to allow for the appropriate provision of services, such as medical and mental health services.[1043]

9.13 The TLRI's view

9.13.1 As noted at [4.15], the TLRI considers that the 'basic personal information' exception in the PIPA should be subject to further consultation to determine its use, effectiveness, and appropriateness in relation to information sharing.

9.13.2 The TLRI agrees with the submissions received in relation to the need for information sharing to be lawful in circumstances where it is necessary on the grounds of safety (such as family violence or child safety). There are several legislative provisions that allow for this in Tasmania. This may be in relation to safety and wellbeing of children, people experiencing family violence, or elder abuse. These are circumstances where there is an exemption to PIPA as 'authorised by law'. This exemption is addressed further in Part 5.

9.13.3 Specifically in relation to information sharing between government agencies, initiatives in other jurisdictions demonstrate the need to ensure a consistent and robust approach to the protection of privacy, while ensuring that government maintains the ability to enhance the value of the information it holds. In some submissions received by the TLRI, concerns were expressed about the absence of an enforceable framework for information sharing within government. In the Tasmanian context, it is the TLRI's view that appropriate privacy safeguards should apply whenever legislation authorises personal information to be shared within and between government agencies and contractors, and that an option would be the introduction of a legislation (such as exists in Victoria, New South Wales, or the Commonwealth) to strengthen the procedures that exist under ADEPT.

9.13.4 As discussed at [9.5.5] above, it is also the TLRI's view that there should be close examination of the relationship between the PIPA and provisions in other Tasmanian legislation with a view to obtaining greater harmonisation and consistency with the provisions of the PIPA. In this regard, the TLRI supports the recommendation of the CoI in relation to the review of legislative barriers to sharing information in the interests of protecting the safety and wellbeing of children and young people.[1044] The TLRI's view is that there is also scope to consider barriers to sharing information within government and, where appropriate, with non-government organisations relating to safety in other contexts, such as family violence, abuse of older people, and persons with a disability.[1045]

9.14 Recommendation

Recommendation 57: The Tasmanian Government should undertake a review of provisions that present legislative barriers to the sharing of information within government and with relevant non-government organisations in the interests of protecting the safety and wellbeing of children and young people, people in family violence situations, abuse of elder persons and persons with a disability.

[1043] Submission 15 (Norma and Carolynn Jamieson).
[1044] See CoI Final Report Recommendations 19.7 and 19.8.

Part 10

Other Legislative Protections of Privacy

10.1 Overview of this Part

10.1.1 In addition to the *Personal Information Protection Act 2004* (Tas) ('PIPA') (discussed in Part 2 of this Report), and the other legislation affecting the privacy of government-held information (discussed in Part 3 of this Report), privacy protections established in Tasmanian legislation apply in several other contexts. These other protections variously deal with information privacy, bodily privacy, privacy of communications, and territorial privacy.

10.1.2 Some of the legislation discussed in this Part provides protection against multiple forms of harm to privacy interests but are generally limited to activities or circumstances in which specific interferences with privacy might occur. These include governmental or workplace surveillance, stalking, harassment, image-based abuse (previously called 'revenge pornography'), and handling of health information.

10.2 Legislative Protections Relating to Surveillance

10.2.1 Surveillance creates a threat to privacy in several ways. It may involve interference with privacy of communications (for example, listening and recording of conversations) and territorial privacy (for example, taking photographs or recording images). Surveillance can be undertaken by government agencies (such as police) or by private individuals or businesses.

The Tasmanian position

10.2.2 Two main Tasmanian pieces of legislation provide protections against unauthorised surveillance: the *Listening Devices Act 1991* (Tas) and the *Police Offences Act 1935* (Tas). They include provisions applying to surveillance that could be undertaken by any person, in any context, and with any device, including Remotely Piloted Aircraft ('RPA') or Unmanned Aerial Vehicles ('UAV'), commonly known as drones.

Listening Devices Act 1991 (Tas)

10.2.3 The prohibitions in the *Listening Devices Act 1991* (Tas) are not limited to state surveillance or to a specific type of device. For example, they also limit how individuals and businesses can record conversations and how people may use drones.

10.2.4 The *Listening Devices Act 1991* (Tas) prohibits the use of listening devices to record private conversations or to listen to private conversations where the person using the device is not a party to it.[1046] There are other offences in relation to communicating or publishing records of private

[1046] *Listening Devices Act 1991* (Tas) s 5(1).

conversations and possession of private conversations.[1047] These offences are punishable by a fine not exceeding 40 penalty units ($7,800) or imprisonment for a term of up to two years or both (for an individual) and a fine not exceeding 500 penalty units ($97,500) for a corporation.[1048] The definition of 'private conversation' is conditioned on 'circumstances that may reasonably be taken to indicate' that the people participating in the conversation intend for it to be heard by others only with their explicit consent.[1049]

10.2.5 Aside from creating offences relating to private conversations, if law enforcement personnel obtain evidence unlawfully under the Act, this limits the circumstances in which the evidence can be used in court.[1050] Even if a recording was lawfully obtained under certain provisions of the Act, any parts that are irrelevant to the commission of serious crimes must be destroyed as soon as practicable.[1051]

10.2.6 While the general rule is a prohibition on the use of listening devices, there are exceptions.[1052] They include:

- warrants issued under the Act for law enforcement activities;[1053]
- the use of a personal camera (as a listening device) by a police officer in the circumstances authorised by legislation;[1054]
- the use of a surveillance device, where authorised by legislation;[1055]
- activities authorised under other legislation, including Commonwealth legislation;[1056]
- unintentional hearing through use of a listening device;
- if a principal party to the conversation consents to the listening device being used and the recording of the conversation is reasonably necessary for the protection of the lawful interests of that principal party;[1057]
- recording interviews between a police officer and a person suspected of having committed a statutory offence;
- where the parties have consented; and

[1047] *Listening Devices Act 1991* (Tas) ss 9, 10 and 11.
[1048] *Listening Devices Act 1991* (Tas) s 12.
[1049] *Listening Devices Act 1991* (Tas) s 3(1).
[1050] *Listening Devices Act 1991* (Tas) pt III.
[1051] *Listening Devices Act 1991* (Tas) s 21.
[1052] *Listening Devices Act 1991* (Tas) ss 5(2)-(7).
[1053] *Listening Devices Act 1991* (Tas) pt IV.
[1054] *Listening Devices Act 1991* (Tas) s 5(2)(bb).
[1055] *Listening Devices Act 1991 (Tas)* s 2(ba).
[1056] *Telecommunications (Interception) Act 1979* (Cth); *Police Powers (Surveillance Devices) Act 2006* (Tas).
[1057] *Listening Devices Act 1991* (Tas) s 5(3)(b)(i). In the Queensland context, in the context of family violence, the following examples are given of when a recording may be to protect a person's lawful interests ('current or continuing abuse and exploitation, contravention of a domestic violence order where the person had a 'genuine concern for their own safety') and not falling within the exception ('where a recording was made to "trap" the other party in engaging in particular conduct where the 'threat of disclosure' of the recording could be used to 'persuade' the other party to take certain action' or where a victim of crime records a conversation with an alleged offender for the purpose of obtaining admissions; however, this will depend on the particular circumstances, including the proximity in time of the offending to the conversation and the victim's ability to take other reasonable action, such as approaching the police': Department of Justice and Attorney-General (Qld), *Civil Surveillance Reforms* (2023) 29.

- where evidence or information needs to be obtained through a listening device in connection with various serious offences or threats.[1058]

10.2.7 Where a listening device is used in connection with a serious offence or threat, a report detailing the use of the device must be provided to the Chief Magistrate within three days.[1059] If the Chief Magistrate is satisfied that it was an unnecessary interference with the privacy of the person whose conversation was listened to, they *may* order that notice be given to that individual.[1060]

10.2.8 In these circumstances, privacy is not always protected through judicial intervention. Rather, privacy merely acts as a precondition before the Chief Magistrate can make an order requiring notice to be given. Even if it was an unnecessary privacy interference, there is no compulsion for notice to be ordered. Further, even if no notice is provided, information obtained in these circumstances is still lawfully obtained.

10.2.9 The *Listening Devices Act 1991* (Tas) also refers to 'privacy' in the context of courts issuing warrants for law enforcement to use listening devices. When determining whether to issue a warrant, a magistrate must have regard to several factors, including the extent to which the privacy of any person is likely to be affected by the surveillance.[1061] The Supreme Court of Tasmania has reiterated that this factor must be considered.[1062] Other factors to be taken into account, and which weigh against the privacy factor, include the evidentiary value of the evidence to be obtained and the nature of the offence.

10.2.10 It should be noted that the *Police Powers (Surveillance Devices) Act 2006* (Tas) further authorises the issuing of police surveillance warrants by the courts, in circumstances where there is a reasonable suspicion or belief of an offence.[1063] Senior officers may also authorise use of a surveillance device in emergency circumstances.[1064] Amendments introduced in 2018 also permit the use of a personal camera by on-duty police officers to record private conversations.[1065] To this extent, this Act permits law enforcement officers to interfere with privacy.

10.2.11 However, under this Act, the power to undertake surveillance under warrants is subject to monitoring, review, and inspection.[1066] Further, the Act limits how the recorded information can be used. Specifically, it makes it an offence to use information obtained through surveillance under the Act, or information relating to warrants or authorisations for surveillance, unless that use is for various specific purposes (listed in the Act).[1067]

Police Offences Act 1935 (Tas)

10.2.12 The *Police Offences Act 1935* (Tas) provides that it is an offence to observe or visually record another person in breach of privacy.[1068] This is another general prohibition on surveillance—in this case, visual observation rather than listening to private conversations. As with offences provided under

[1058] For example, serious narcotics offences or an imminent threat of serious violence to persons or of substantial damage to property: *Listening Devices Act 1991* (Tas) s 5(2)(c).
[1059] *Listening Devices Act 1991* (Tas) s 5(4); see also s 5(7).
[1060] *Listening Devices Act 1991* (Tas) s 6(2).
[1061] *Listening Devices Act 1991* (Tas) s 17(2).
[1062] *Kirkland v Tippett* [2000] TASSC 94 (19 July 2000).
[1063] *Police Powers (Surveillance Devices) Act 2006* (Tas) s 9.
[1064] *Police Powers (Surveillance Devices) Act 2006* (Tas) pt 3.
[1065] *Surveillance Legislation Amendments (Personal Police Cameras) Act 2018* (Tas).
[1066] *Police Powers (Surveillance Devices) Act 2006* (Tas) pt 5.
[1067] *Police Powers (Surveillance Devices) Act 2006* (Tas) ss 32–3.
[1068] *Police Offences Act 1935* (Tas) s 13A(1).

the *Listening Devices Act 1991* (Tas), the offence is not limited to any specific type of device and would cover the use of drones (discussed further at [10.2.18] below).

10.2.13 The offence is limited to observing or visually recording a person 'in circumstances where a reasonable person would expect to be afforded privacy'. The recording must be done without that person's consent *and* when that person is either: (1) in a private place; or (2) engaging in a private act and the recording is made for the purpose of observing or visually recording a private act. The maximum penalty is 12 months' imprisonment and/or 50 penalty units.

10.2.14 This offence has been held by the Supreme Court to be a 'reportable offence' within the meaning of Section 6(1) the *Community Protection (Offender Reporting) Act 2005* (Tas).[1069] In essence, the effect of this classification is that offenders may be ordered to keep police informed of their whereabouts and other personal details for a period of time.

10.2.15 Closely related to this offence, the *Police Offences Act 1935* (Tas) also makes it an offence to:

- possess a prohibited visual recording;[1070]
- publish or distribute such a recording;[1071] and
- observe or visually record another person's genital or anal region, in circumstances where a reasonable person would expect to be afforded privacy in relation to that region, and where it is done for the purpose of observing or visually recording the other person's genital or anal region (a specialised version of the general observing or recording offence, which carries a defence of consent).[1072]

10.2.16 Regarding this range of offences of observing and recording in breach of privacy, there are more limited exceptions than exist under the *Listening Devices Act 1991* (Tas), with three categories of people only excluded from criminal responsibility, provided that they meet the onus of proving that they fall within one of thee categories. They are as follows:[1073]

- a law enforcement officer acting reasonably in the course of performing their duties;
- a person acting reasonably in the course of their duties in relation to someone who is in lawful custody (for example, officers in prisons); and
- a person acting in the course of their occupation or employment and where their conduct is reasonable in that context.

10.2.17 In essence, people who fall within these three categories are lawfully permitted to interfere with individuals' privacy through observation or visual recording.

Drones

10.2.18 Tasmania does not have specific regulations that limit how RPAs or UVAs (drones) can interfere with privacy. However, as noted above, drones are encompassed within the general criminal prohibitions on the use of listening devices and on observing or visually recording people. Surveillance

[1069] *Hickman v PWJ* [2015] TASSC 55 (20 November 2015). This is a recent case in which the respondent was found guilty of the offence of observation and recording, contrary to *Police Offences Act 1935* (Tas) s 13A(1).
[1070] *Police Offences Act 1935* (Tas) s 13C.
[1071] *Police Offences Act 1935* (Tas) s 13B.
[1072] *Police Offences Act 1935* (Tas) s 13A(2).
[1073] *Police Offences Act 1935* (Tas) s 13D.

by a drone may also give rise to an offence of stalking or harassment (see [10.7.7] below). Personal information captured by a drone would also be subject to obligations under the Tasmanian *Personal Information Protection Act 2004* (Tas) ('PIPA') or the Commonwealth *Privacy Act 1988* (Cth) ('Privacy Act'). Drones may also be subject to limitations in the law of civil wrongs; specifically, nuisance and trespass. For example, in the case of nuisance, a drone operator could be found liable where they cause persistent and continuing interference with use and enjoyment of property.

10.2.19 At the Commonwealth level, drones are considered 'aircraft' under the *Civil Aviation Act 1988* (Cth) and are subject to control by the Civil Aviation Safety Authority. The regulations include restrictions on the flying of drones over populous areas, including private property.[1074] However, there are no legislative limitations that explicitly and specifically relate to privacy.

The position in other jurisdictions

10.2.20 In other jurisdictions (as with Tasmania), there are other statutes that apply to the issue of surveillance using listening devices and cameras.[1075] In contrast to Tasmania, however, the scope of the legislation in other States and Territories (with the exception of the ACT and Queensland) applies more broadly than just to listening devices and extends to optical surveillance devices, tracking devices, and, in some cases, data surveillance devices.[1076]

10.2.21 In New South Wales, Victoria, and the ACT, unlike Tasmania, there are also specific laws that apply to surveillance and monitoring of employees by employers.[1077] Reforms have been proposed to the legislation that exists in New South Wales. In 2022, a report released by the Select Committee on the Impact of Technological and Other Change on the Future of Work and Workers in New South Wales outlined the various forms of electronic monitoring and surveillance that may take place in a workplace, including through biometrics, closed circuit television ('CCTV'), and location tracking.[1078] It made recommendations to build into workplace surveillance laws clear privacy protections and the requirement for external approval prior to undertaking or implementing workplace surveillance measures.[1079] Consultation in relation to the introduction of a provision to specifically regulate the surveillance of employees by employers using surveillance devices is currently underway in Queensland.[1080]

10.2.22 In addition to workplace surveillance, a Queensland review is examining the expansion of the laws to regulate surveillance by an optical device, a tracking device, and a data surveillance device, in addition to listening devices.[1081] This consultation builds upon the Queensland Law Reform Commission's 2020 report, which made recommendations for new legislation to appropriately protect

[1074] See, eg, *Civil Aviation Safety Regulations 1998* (Cth) ss 101.025, 101.055.
[1075] See summary provided at Department of Infrastructure, Transport, Regional Development, Communications and the Arts, Drones: Privacy Policy <https://www.drones.gov.au/policies-and-programs/policies/privacy-policy>. It is noted that the *Surveillance Devices Act 2004* (Cth) applies to the use of surveillance devices by agencies, including State and Territory law enforcement agencies when they are using surveillance devices under Commonwealth Laws.
[1076] See discussion in Department of Justice and Attorney-General (Qld), *Civil Surveillance Reforms* (2023) 9–11.
[1077] *Workplace Surveillance Act 2005* (NSW); *Surveillance Devices Act 1999* (Vic) pt 2A; *Workplace Privacy Act 2011* (ACT).
[1078] Select Committee on the Impact of Technological and Other Change on the Future of Work and Workers in New South Wales, *Impact of Technological and Other Change on the Future of Work and Workers in New South Wales: Final Report – Workplace Surveillance and Automation*, Report 22 (November 2022) 11.
[1079] Ibid Recommendations 2, 5.
[1080] Department of Justice and Attorney-General (Qld), *Civil Surveillance Reforms* 44–45.
[1081] Ibid.

the privacy of individuals in the context of civil surveillance technologies.[1082] The Queensland review also highlights technology facilitated surveillance of a victim as one of a number of controlling behaviours that may exist in the context of family violence.[1083]

10.2.23 Concerns about the use of digital surveillance and the adequacy of the law has arisen in the context of family violence. For example, its potential as a tool for the perpetration of family violence has been recognised in the *National Domestic and Family Violence Bench Book*,[1084] which highlights the covert and overt use of technology as an aspect of a pattern of behaviour in coercive control. The *Bench Book* also stresses the need to distinguish between behaviour where the victim uses digital technology as a protective means to prevent or escape family violence (for example, where the victim records repeated incidents of violence) and behaviours that constitute violence by the perpetrators.

10.3 The Commonwealth Privacy Act Review

10.3.1 As discussed in Part 11 of this Report, the Commonwealth Privacy Act Review gave consideration to the creation of a statutory tort for serious invasion of privacy,[1085] which would apply to invasions of privacy more broadly than surveillance through listening devices or drones.[1086] The Government agreed in-principle to the creation of a statutory tort for serious invasions of privacy.[1087] The Privacy Act Review also made other recommendations about the regulation of the handling of biometric data that would operate in the context of workplace surveillance.[1088]

10.3.2 Other developments initiated by the Commonwealth Government include the consultation paper published by Department of Infrastructure, Transport, Regional Development, Communications and the Arts, seeking public submissions on drone privacy guidelines. It notes that there are 'unique potential impacts of drone use on privacy, and the heightened community sensitivity to the use of drones in areas where there is a reasonable expectation of privacy'.[1089] The proposed guidelines 'consider relevant Australian privacy and surveillance legislation to provide commercial and recreational drone operators with a set of consolidated, easy to follow, baseline measure for operating drones in line with privacy expectations'.[1090] Major reforms of Australia's electronic surveillance framework are also being developed, which will include repeal of the *Surveillance Devices Act 2004* (Cth). This follows the review of the legal framework conducted by Dennis Richardson AC.[1091]

[1082] Queensland Law Reform Commission, *Review of Queensland's law relating to Civil Surveillance and the Protection of Privacy in the Context of Current and Emerging Technology*, Report 77 (2020).
[1083] Department of Justice and Attorney-General (Qld), *Civil Surveillance Reforms* 8. See also Women's Safety and Justice Taskforce, *Hear Her Voice: Report One – Addressing Coercive Control and Domestic and Family Violence in Queensland* (2022).
[1084] *National Domestic and Family Violence Bench Book: Following, Harassing and Monitoring* (2023) <https://dfvbenchbook.aija.org.au/understanding-domestic-and-family-violence/following-harassing-and-monitoring/>.
[1085] See discussion at [11.4].
[1086] See discussion at [11.4.2].
[1087] Australian Government, *Government Response to the Privacy Act Review Report* (2023) 19.
[1088] See discussion at [4.8].
[1089] Department of Infrastructure, *Don't Pry When You Fly: Privacy Considerations for Drone Use* (Commonwealth of Australia, 2023) 6.
[1090] Ibid 5.
[1091] See Attorney-General's Department, *Reform of Australia's Electronic Surveillance Framework* <https://www.ag.gov.au/crime/telecommunications-interception-and-surveillance/reform-australias-electronic-surveillance-framework>; D Richardson, *The Comprehensive Review of the Legal Framework of the National Intelligence Community* (2019) <https://www.ag.gov.au/national-security/consultations/comprehensive-review-legal-framework-governing-national-intelligence-community>.

10.4 Consultation

10.4.1 The TLRI Issues Paper invited submissions on the protection of privacy in the context of surveillance in response to the following questions:

> Should the existing protections in the listening devices legislation be amended in Tasmania to strengthen the protection of individuals against surveillance, whether governmental, workplace, or private surveillance?[1092]
>
> Should there be stronger legislative protection, including through the introduction of new statutes in Tasmania, against governmental (particularly police) surveillance in general?[1093]
>
> Should there be stronger legislative protection, including through the introduction of new statutes in Tasmania, against workplace surveillance in particular?[1094]
>
> Should there be specific protection against interference with physical privacy through the use of drones (RPAs and UAVs)?[1095]

10.4.2 The adequacy of *Listening Devices Act 1991* (Tas) as a means to protect individuals against surveillance was addressed by Meg Webb MLC, who expressed the view that the existing protections should be strengthened.

10.4.3 The need for a nuanced and comprehensive legislative approach under the *Listening Devices Act 1991* (Tas) and other criminal offences applying to surveillance was seen to be necessary by Tasmanian Legal Aid ('TLA') to allow the law to respond to issues that arise in the family violence context. TLA reported that surveillance is 'a double-edged sword'. TLA stated that surveillance may be protective in circumstances such as where a victim of family violence surreptitiously records a handover of their child to the other, sometimes abusive, parent, where there is opportunity for, and risk of, verbal abuse and/or threats of violence, or makes a known but unwanted recording that is an effective curb on the offender's abusive behaviour. On the other hand, surveillance may be intimidating and part of a pattern of coercive control. TLA provided the example of a situation where a family violence offender overtly records the victim of family violence at handover of the child, whilst berating her about parenting, in the context of threat to report the victim to Child Safety Services.

10.4.4 Another theme in the responses was the scope of surveillance powers for police.

10.4.5 Tasmania Police provided detailed comment on the legislative framework that supports the covert policing techniques and tools used, which Tasmania Police recognised may have an effect on personal privacy protection. Tasmania Police submitted that striking the right balance between competing interests of individual privacy and public safety was complex and presented an ongoing challenge. However, Tasmania Police highlighted the protections and safeguards that exist under the *Listening Devices Act 1991* (Tas) and the *Police Powers (Surveillance Devices) Act 2006* (Tas) through the use of warrants issued by judicial officers and the imposition of reporting requirements to the Chief Magistrate and the Attorney-General, and the rules of evidence that allow for improperly or illegally obtained evidence to be excluded from a criminal trial under Section 138 of the *Evidence Act 2001* (Tas). Tasmania Police noted that independent oversight of the legislated powers was administered by the Department of Justice, and further that, under the *Ombudsman Act 1978* (Tas), Tasmania Police is

[1092] Issues Paper Part 4, Question 4.1.
[1093] Ibid Part 4, Question 4.2.
[1094] Ibid Part 4, Question 4.3.
[1095] Ibid Part 4, Question 4.4.

accountable to the Tasmanian Ombudsman for any breach of privacy under legislation.[1096] Oversight is also provided by recourse to Tasmania Police's Professional Standards complaint mechanisms.

10.4.6 Tasmania Police outlined potential challenges to police operations. if privacy protections were increased within the legislative framework:

1. *Impaired investigation efforts*: strengthening privacy protection measures may limit the amount and type of information available to Tasmania Police. This may restrict access to certain data sources or require additional legal steps, slowing down investigations, potentially compromising public safety.

2. *Delayed response times*: there may be delays in obtaining necessary warrants to access data.

3. *Weakening surveillance techniques*: curtailing the use of certain surveillance techniques that rely on collecting and analysing personal data (e.g., restrictions on monitoring online communications, or tracking individuals' activities through mobile devices).

4. *Hindering information sharing*: limiting sharing of information between Tasmania Police and other Australian agencies or intelligence organisations.

5. *Increased burden on resources*: enhancing privacy protections often necessitates additional resources, such as advanced technologies, personnel training, and compliance measures.

6. *Evolving criminal tactics*: sophisticated offenders are likely to adopt enhanced privacy protections and exploit them to their advantage.

10.4.7 Tasmania Police wrote that:

> In summary, the current legislative framework requires Tasmania Police to meet threshold requirements for obtaining a warrant to use listening devices and other surveillance methods. The legislation that Tasmania Police operates under is subject to review and reform by the Department of Justice. And finally, Tasmania Police members are accountable to both the Tasmania Police Professional Standards command and the Tasmanian Ombudsman for any complaints of breaches of privacy.

10.4.8 In contrast, the Tasmanian Council of Social Service ('TasCOSS') expressed the view that there was a need for stronger protection against police surveillance and privacy breaches,[1097] and that independent oversight of police decisions was particularly important in relation to police interactions with marginalised groups. TasCOSS stated that '[p]olice have significant powers which can, in certain circumstances, directly and significantly impact on the privacy of an individual family or community' and that currently there was limited oversight of how police exercise their powers. TasCOSS stated that most complaints are dealt with internally and the possibility of external review by the Ombudsman or the Integrity Commission was impeded by a lack of capacity and resourcing to effectively investigate or respond to complaints.

10.4.9 TasCOSS's stated that independent oversight of police complaints is needed to safeguard both the rights of Tasmanians and the integrity of the police service and pointed to the approach suggested

[1096] See *Ombudsman Act 1978* (Tas) Div 3.
[1097] TasCOSS referred to concerns about potential privacy breaches through the use of listening devices and surveillance equipment by Tasmania Police at Risdon Prison.

by some community organisations in Victoria for the introduction of a specialist police ombudsman. Such an ombudsman could have the following characteristics:

- institutional independence;
- adequately resourced to appropriately respond to complaints;
- complainant-centred and culturally appropriate;
- fair, accountable, and transparent;
- ability to achieve timely and fair outcomes; and
- ability to promote systemic change.

10.4.10 TasCOSS indicated that it would support the introduction of an independent entity with similar characteristics in Tasmania and strongly recommended legislative and other policy mechanisms to enhance police accountability.

10.4.11 Meg Webb MLC also supported stronger legislative protections against governmental (particularly police) surveillance, which would include greater independent transparency, assessment, and reporting mechanisms, as well as appeal rights.

10.4.12 The Commissioner for Children and Young People expressed concerns in relation to the use of body worn cameras by police in relation to children, particularly concerning the storage and access to those materials in the future.

10.4.13 In response to the question relating to need for specific protection against interference with physical privacy through the use of drones (RPAs and UAVs), two submissions expressed the view that such reform was necessary.[1098] Meg Webb MLC stated that 'these forms of technology can be applied in an indiscriminatory manner which can have serious implications for minors and other vulnerable members of the community'.

10.5 The TLRI's view

10.5.1 In relation to the issue of the adequacy of the surveillance legislation applying in Tasmania (see [10.2]), the TLRI notes that, generally, the approach under the *Listening Devices Act 1991* (Tas) and the *Police Offences Act 1935* (Tas) provide a broad safeguard for individual privacy. This is achieved by protecting people from surveillance though the recording of private conversations or taking of images in circumstances where a person would expect to be afforded privacy. Although not specifically referring to drones, as noted, this legislation would extend to the use of a drone to record a private conversation or to record an image of a private act. Nevertheless, the TLRI considers that there is scope to expand existing surveillance protections contained in the *Listening Devices Act 1991* (Tas) to cover a broader range of technologies (such as visual and tracking devices), as exists in most other jurisdictions. It is noted that, while the recording of images is captured under the *Police Offences Act 1935* (Tas), the TLRI's view is that consideration should be given to reform of the protection in the listening devices legislation to strengthen protections for individuals against surveillance by optical surveillance devices, tracking devices, and data surveillance devices.

10.5.2 The TLRI notes that there is a range of safeguards in relation to the powers of police to use surveillance devices. As discussed at [10.2.6] above, law enforcement exceptions to the *Listening*

[1098] Submission 8 (Meg Webb MLC); Submission 3 (Anonymous).

Devices Act 1991 (Tas) apply in relation to warrants, recording interviews between a police officer and a person suspected of having committed an offence, and in cases where evidence of information needs to be obtained in connection with various serious offences. Oversight is provided through the requirement to obtain a warrant, or by review by the Chief Magistrate in cases of serious offences. In relation to both surveillance pursuant to a warrant or in cases where a listening device is used in connection with an imminent threat of serious violence to person or of substantial damage to property or a serious narcotics offence, the *Listening Devices Act 1991* (Tas) requires a report to be made to the Attorney-General.[1099] The Attorney-General is required to have a report prepared in relation to the number of warrants sought and granted, and for that report to be laid before Parliament.[1100]

10.5.3 There is also a requirement under the *Police Powers (Surveillance Devices) Act* 2006 (Tas) for reports to be made to the Supreme Court or Magistrates Court in relation to the execution of a surveillance device warrant or a retrieval warrant.[1101] Police are also required to keep records connected with warrants and the register is to be inspected by an independent person as an inspection entity at least once every 12 months; this report must be provided to the relevant minister and laid before Parliament. Annual reports to the Minister about the use of warrants are also required;[1102] The rules of evidence under the *Evidence Act 2001* (Tas) and the restrictions of the admissibility of evidence under the *Listening Devices Act 1991* (Tas) Part 3.[1103] Oversight is also provided the Ombudsman.

10.5.4 While consideration could be given to the establishment of a specialist police ombudsman to provide oversight to the use of surveillance by Tasmania Police, as suggested by TasCOSS, the TLRI's view is that a range of safeguards and oversight already exist, including oversight by the Ombudsman and the requirement for reports to be tabled in Parliament. Accordingly, the TLRI's view is that it is not necessary to make changes to the legislative framework at this time. However, consideration should be given to improving the resources made available to allow for independent monitoring of police use of surveillance devices by the Ombudsman.

10.6 Recommendations

Recommendation 58: Consideration should be given to reform of the listening devices legislation to strengthen protections for individuals against surveillance by optical surveillance devices, tracking devices, and data surveillance devices.

Recommendation 59: Consideration should be given to improving the resources made available to allow for independent monitoring of police use of surveillance devices by the Ombudsman.

[1099] *Listening Devices Act 1991* (Tas) ss 8 and 19.
[1100] *Listening Devices Act 1991* (Tas) s 22.
[1101] *Police Powers (Surveillance Devices) Act 2006* (Tas) s 29
[1102] *Police Powers (Surveillance Devices) Act 2006* (Tas) s 44.
[1103] See, eg, *Tasmania v Thompson* [2022] TASSC 53, *Tasmania v Thompson (No 2)* [2022] TASSC 55. The use of police surveillance in this case is the subject of an independent review: see Tasmanian Government, *Review of the Use of Surveillance Devices in Prisons: Terms of Reference* (2022) <https://www.police.tas.gov.au/uploads/Review-of-Surveillance-Devicesin-Prisons-Terms-of-Reference-November-2022.pdf>; see also [10.5].

10.7 Legislative protections relating to stalking and harassment

10.7.1 Stalking, harassment, and bullying may in some circumstances involve interference with privacy—whether through intrusion upon seclusion (also referred to as physical privacy, meaning a person's bodily or territorial privacy), or through the malicious use of private information against the person concerned (for example, to intimidate, blackmail, or otherwise coerce that person). As with other egregious interferences with privacy, these behaviours may cause humiliation, psychological distress, or intimidation.[1104]

The Tasmanian position

10.7.2 In Tasmania, various legislation prohibits stalking and similar behaviour. Where stalking or bullying that is already proscribed in law involves an interference with privacy, existing legislation may provide protection and redress for the privacy-related harm. However, there is no legislation specifically orientated towards protecting physical or information privacy against interferences by behaviour involving stalking and bullying. For example, it is not a specific offence under Section 192 of the *Criminal Code* (Tas) to intimidate or harass a person separately from where such conduct would amount to stalking or bullying. Further, there is no specific Tasmania legislation that relates to the sharing of intimate images that were initially taken with consent and then later shared (or threatened to be shared) without consent.[1105] Such conduct could come within the scope of the crime of stalking and bullying or child abuse material, if the victim is a minor. It may also be an offence under Commonwealth legislation.[1106]

10.7.3 It is a crime to stalk or bully someone with intent to cause them physical or mental harm, including self-harm, or extreme humiliation, or to be apprehensive or fearful.[1107] The Director of Public Prosecutions must consent before a prosecution for this offence can be commenced.[1108] Stalking or bullying means pursuing a course of conduct involving one or more behaviours listed in the provision.[1109] These include following a person, keeping a person under surveillance, loitering outside a person's residence, using the internet in an intimidating way, and acting in any another way that could reasonably be expected to cause another person the requisite physical or mental harm.

10.7.4 Although this crime covers a reasonably wide range of behaviours that could amount to interference with physical or information privacy and associated harms, there are limits on the extent of privacy protection this provision can achieve. Some difficulties include:

- Even if someone has allegedly engaged in the proscribed behaviour, there may be insufficient evidence to proceed to prosecution.
- A finding of guilt requires a high criminal standard of proof—beyond reasonable doubt.

[1104] See a current governmental review of laws applicable to stalking, harassment, and similar conduct, conducted by the Victorian Law Reform Commission: Victorian Law Reform Commission, *Stalking: Consultation Paper – Terms of Reference* (Web Page, 18 February 2021) <https://www.lawreform.vic.gov.au/publication/stalking-2/terms-of-reference/>; Victorian Law Reform Commission, *Stalking* (Consultation Paper, 24 June 2021).
[1105] See [10.12].
[1106] See [10.12.4].
[1107] *Criminal Code* (Tas) s 192.
[1108] *Criminal Code* (Tas) s 192(6). This can also be tried summarily with the consent of the prosecutor, see *Justices Act 1959* (Tas) s 72(4).
[1109] See discussion in the Director of Public Prosecutions (Tas), *DPP Prosecution Guidelines* 99–100 <https://www.dpp.tas.gov.au/__data/assets/pdf_file/0011/681167/DPP-prosecution-guidelines_v9.pdf> ('DPP Guidelines').

- Even if prosecution is commenced and there is a finding of guilt, it will not necessarily result in any remedies for the victim commensurable to those available under civil law. Criminal law specifies that sentences may be imposed to achieve certain purposes, including punishment, deterrence, and rehabilitation of the perpetrator, and community protection—it does not seek to compensate the victim for harm.
- The requirement that there be a 'course of conduct' means the behaviour must have occurred more than once—one-off instances of intrusion are excluded.[1110]
- The offence requires the prosecutor to prove that the defendant knew that the course of conduct would be likely to cause the specific harm. Depending on the available evidence in any one case, it could be difficult for a prosecutor to prove this 'mental element' of knowledge.[1111]
- The Director of Public Prosecutions Guidelines provide that consent to charge with stalking and bullying (as distinct from pursuing individual charges or preventative courts orders, such as a family violence or restraining orders) will only be given where the course of conduct is extremely serious, the course of conduct has continued over an extensive period of time and lesser charges, restraint orders, or other proceedings have failed to stop the conduct.[1112]

10.7.5 Apart from this general crime, other legislative or regulatory provisions prohibit harassment or similar behaviour in various specific contexts which may involve interferences with privacy. This includes: family relationships;[1113] solicitors' conduct when engaging in court processes (particularly regarding how clients are advised and witnesses are treated);[1114] and public transport.[1115]

10.7.6 Further, the *Anti-Discrimination Act 1998* (Tas) prohibits conduct which offends, humiliates, intimidates, insults, or ridicules another person on the basis of a specified attribute, where a reasonable person would have anticipated the conduct to have that effect on the other person.[1116] Specified attributes include gender, marital status, pregnancy, parental status, and family responsibilities. Given that these relate largely to a person's private and family life, this provision may protect individuals from harmful interferences with their private and family lives, or from misuse of their private information. However, the harmful conduct must be done on the requisite discriminatory basis and with the required intent in order to fall within the scope of this prohibition.

[1110] *Criminal Code* (Tas) s 192(2).
[1111] In this context, 'knowledge' refers to what the defendant actually knew, or what they ought to have known. See also ibid s 13.
[1112] DPP Guidelines 99. Other relevant considerations include the number and type of incidents, the period of time over which the incidents have occurred, the planning and motivation for the conduct, whether individual charges or other court measure have failed to stop the assault, did other serious crimes occur such as sexual assault or the distribution of child exploitation material, the effect the conduct has had on the complainant and whether there is another remedy such as a complaint to the Anti-Discrimination Commissioner or to an employer or school that is taking disciplinary action: see ibid 100.
[1113] *Family Violence Act 2004* (Tas) ss 14(3)(d)–(f), s 16.
[1114] *Legal Profession (Solicitors Conduct) Rules 2000* (Tas) regs 26(1)(c), (2)(c), (8)(a)(ii).
[1115] *Passenger Transport Regulations 2000* (Tas) regs 20(2)(b)–(d).
[1116] *Anti-Discrimination Act 1998* (Tas) s 17(1).

The position in other jurisdictions

10.7.7 Criminal offences that exist in other jurisdictions in relation to stalking are generally consistent with Tasmanian legislation.[1117] However, there are some key differences to the legislative approach in Tasmania that appear to provide for broader protection for surveillance by technology or at least greater clarity around the criminalisation of this type of activity in some other jurisdictions.

10.7.8 The crime of 'unlawful stalking, intimidation, harassment or abuse' in Queensland can be committed by conduct that is engaged in on one occasion if the conduct is protracted, or on more than one occasion.[1118] The crime includes a list of conduct constitutes 'stalking, intimidation, harassment or abuse'.[1119] Recent reforms in Queensland have changed the offence to criminalise surveillance conduct which would constitute an act of stalking; for example, by installing tracking and spyware applications on mobile phones, electronic devices, and vehicles, as well as installing covert cameras and the use of drones.[1120] It would also include publishing offensive material online.

10.7.9 In New South Wales, the equivalent legislation makes it an offence to stalk or intimidate with an intent to cause fear of physical or mental harm.[1121] Stalking is defined to include: following a person; watching or frequenting the vicinity of, or an approach to, a person's place of residence, business, or work or any place that a person frequents for the purposes of any social or leisure activity; or contacting or otherwise approaching a person using the internet or any other technologically assisted means.[1122] Intimidation is defined to include 'conduct (including cyberbullying) amounting to harassment or molestation of the person, or ... an approach by any means (including by telephone, telephone text messaging, e-mailing and other technologically assisted means) that causes the person to fear for his or her safety'.[1123]In addition to criminal offences, in other jurisdictions such as New South Wales, Queensland, and Victoria, there are equivalent orders to family violence orders or restraint orders that exist in Tasmania.[1124] However, unlike in Tasmania, harassment has been specifically recognised in these jurisdictions as emotional or psychological abuse and/or intimidation in some jurisdictions and so provides a clear basis for making a protective order.[1125]

10.8 The Commonwealth Privacy Act Review

10.8.1 As discussed in Part 11, the Commonwealth Privacy Act Review considered the creation of a statutory tort for serious invasion of privacy, and while some conduct amounting to harassment and

[1117] See, eg, *Crimes Act 1900* (ACT) s 35; *Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13; *Criminal Code* (NT) s 189*; Criminal Code 1899* (Qld) Ch 33A; *Criminal Law Consolidation Act 1935* (SA) s 19AA; *Crimes Act* (Vic) s 21A; *Criminal Code* (WA) s 338E.
[1118] *Criminal Code 1899* (Qld) s 359B(b).
[1119] See *Criminal Code 1899* (Qld) s 359B(c).
[1120] See *Criminal Code 1899* (Qld) s 359B(c)(iv).
[1121] *Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 13.
[1122] *Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 8(1).
[1123] *Crimes (Domestic and Personal Violence) Act 2007* (NSW) ss 7, 13.
[1124] See, eg, *Crimes (Domestic and Personal Violence) Act 2007* (NSW) pts 4 and 5; *Domestic and Family Violence Protection Act 2012* (Qld); *Personal Safety Intervention Orders Act 2010* (Vic); *Family Violence Protection Act 2008* (Vic).
[1125] See, eg, *Domestic and Family Violence Protection Act 2012* (Qld) s 11; *Crimes (Domestic and Personal Violence) Act 2007* (NSW) s 7; *Family Violence Protection Act 2008* (Vic) s 7; *Family Violence Act 2016* (ACT) s 8(3); *Restraining Orders Act 19991* (WA) s 5A; *Domestic and Family Violence Act 2007* (NT) ss 5, 6. It is noted that in Tasmania, a police family violence may require a person to refrain from harassing (as defined in s 4) another person: *Family Violence Act 2004* (Tas) see s 14(3)(a). However, harassment is not specifically included as an order that can be made in relation to the making of a Family Violence Order: ibid see s 16.

stalking may give rise to a serious invasion of privacy, this was not addressed as a separate issue. As noted, the Government gave in-principle agreement to the creation of a statutory tort.[1126]

10.9 Consultation

10.9.1 The TLRI Issues Paper invited submissions on privacy in the context of stalking and harassment in response to the following question:

> Are the existing legislative protections against stalking and harassment adequate to protect physical privacy, or should there be a new or strengthened law to protect against such physical and intimidating interferences?[1127]

10.9.2 This issue was addressed in three submissions, with the responses indicating that the current protections were inadequate.[1128] TLA addressed the issue of privacy in the context of family violence and observed that stalking and harassing behaviours are not frequently prosecuted and may not be recognised as family violence or breach of an order when reported to police. TLA noted that '[a]necdotally, clients frequently report harassing or stalking behaviour to police but are informed that it is "not stalking" or "not enough"'. TLA stated that this was potentially exacerbated by current understandings and practices in relation to family violence orders, following the Magistrates Court decision in *Howe v S*,[1129] about the meaning of 'harassment', which resulted in harassment being removed from the standard orders available on family violence orders. Accordingly, TLA agreed with the Issues Paper that the current stalking and harassing provisions and/or practices may be inadequate to protect victims from surveillance, stalking and harassment.

10.10 The TLRI's view

10.10.1 After reviewing the legislation that exists in other jurisdictions and taking into account the submissions received, the TLRI's view is that there are areas in which the criminal laws that apply in relation to stalking and bullying could be strengthened in Tasmania to provide greater clarity around, and better protection for, physical privacy; changes may also be required to the conduct that may give rise to a family violence order being made.[1130] While stalking and harassment can encompass a range of behaviours, the Australian Institute of Health and Welfare has recognised that 'the widespread availability of technology and the ease of maintaining anonymity online has increased the opportunity for stalking and surveillance in recent years. Perpetrators may misuse devices, accounts, software or platforms to control, abuse and track victim-survivors'.[1131]

10.10.2 The adequacy of the existing laws relating to stalking and intimidation in Tasmania and the need to amend the laws to take better account of technological advances should be the subject of review in Tasmania. Key changes that could be considered include:

[1126] Government Response 19.
[1127] Issues Paper Part 4, Question 4.5.
[1128] Submission 8 (Meg Webb MLC); Submission 3 (Anonymous); Submission 5 (TLA).
[1129] *Howe v S* [2013] TASMC 33.
[1130] It is noted that, in Part 11, the TLRI also discusses the creation of a tort for the invasion of privacy that would provide a civil remedy that may apply in some of these situations.
[1131] AIHW, *Stalking and Surveillance* (Web Page, 12 April 2024) <https://www.aihw.gov.au/family-domestic-and-sexual-violence/types-of-violence/stalking-surveillance>.

- Reforming the crime of stalking and bullying in the *Criminal Code* (Tas) s 192 to also include intimidation based on the New South Wales approach, with intimidation defined separately from stalking, and changing the provision to recognise that a pattern of behaviour may be taken into account in the determination of stalking or intimidation, so that it does not specify that there has to be more than one act.
- Reviewing the extent to which behaviour that amounts to harassment is adequately protected for the purposes of the *Family Violence Act 2003* (Tas).
- Amending the crime of stalking and bullying in the *Criminal Code* (Tas) s 192 to more clearly criminalise surveillance conducted by technology; for example, by installing tracking and spyware applications on mobile phones, electronic devices and vehicles, as well as installing covert cameras and the use of drones.

10.11 Recommendation

Recommendation 60:

A review should be conducted that examines the adequacy of the existing laws relating to stalking and intimidation in Tasmania and that considers whether there is a need to amend these laws to take better account of technological advances. The following could be considered in the review:

- whether the crime of stalking and bullying in the *Criminal Code* (Tas) Section 192 should be amended to include intimidation based on the New South Wales approach—with intimidation being defined separately from stalking—and the provision should be changed to recognise that a single act, or a pattern of behaviour, may be taken into account in the determination of stalking or intimidation;
- the extent to which behaviour that amounts to harassment is adequately protected for the purposes of the *Family Violence Act 2003* (Tas); and
- whether the crime of stalking and bullying in the *Criminal Code* (Tas) Section 192 should be amended to more clearly criminalise surveillance conducted by technology; for example, by installing tracking and spyware applications on mobile phones, electronic devices, and vehicles, as well as installing covert cameras and the use of drones.

10.12 Unauthorised sharing of intimate images

10.12.1 The unauthorised sharing of intimate images is also described as 'image-based abuse' or, colloquially, 'revenge porn'. Australian research suggests that image-based sexual abuse is relatively common (reported by one in five respondents) and disproportionately affects Aboriginal and Torres Strait Islander people, people with a disability, homosexual and bisexual people, and young people.[1132] As acknowledged by the eSafety Commissioner, it is 'generally intended to cause harm, distress, humiliation and embarrassment' and may be done 'in an attempt to control, coerce, "punish" or blackmail the target of the image-based abuse'.[1133] The unauthorised or non-consensual sharing of intimate images covers a broad range of conduct, including images that were: initially taken with consent or by the person themselves and later shared without consent; shared initially with consent and then later shared without consent; or obtained without consent, such as from online sites or through the

[1132] Nicola Henry, Asher Flynn and Anastasia Powell 'Image-based Sexual Abuse: Victims and Perpetrators' (2019) 572 *Trends and Issues in Criminal Justice* 1, 10.
[1133] eSafety Commissioner, *Image-Based Abuse Scheme Regulatory Guidance: eSC RG 2* (2021) 4.

use of hidden recording device, and then distributed.[1134] It may also include doctored images (including intimate 'deepfake images' created using generative artificial intelligence).[1135] Research suggests that there can be serious and harmful consequences for the targets of such abuse.[1136] However, regardless of the harm, it also amounts to a breach of an individual's 'fundamental rights to dignity and privacy, as well as their freedom of sexual expression and autonomy'.[1137]

The Tasmanian position

10.12.2 In Tasmania, there is no specific Tasmanian law concerning image-based abuse. However, an offence may be committed under the *Police Offences Act 1935* (Tas), if a person publishes or distributes a recording made without consent and when the person is in a private place or engaging in a private act.[1138] This offence does not apply if the recording was made with consent but is subsequently published or distributed without consent. However, it is a crime under Commonwealth laws to share private sexual images online without consent.[1139] These Commonwealth offences apply in Tasmania. If the images involve people under the age of 18, then the conduct may also fall under child sexual exploitation material.

10.12.3 While an attempt was made to introduce an offence of image-based abuse, and associated remedies, in 2017, the *Civil Digital Communications Bill 2017* (Tas) did not progress past its First Reading in the House of Assembly.[1140]

The position in other jurisdictions

10.12.4 At the Commonwealth level (and applying in Tasmania), the *Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018* (Cth) amended the *Criminal Code Act 1995* (Cth) to provide for an aggravated version of the existing offence of using a carriage service to menace, harass, or cause offence.[1141] The aggravated offence applies where commission of the underlying offence involves transmitting, making available, publishing, distributing, advertising, or promoting private sexual material. This amendment is largely targeted at image-based abuse, which involves the non-consensual online publication of intimate sexual images of an individual, usually with the intent or effect of harassing, blackmailing, shaming, or demeaning them.

10.12.5 There is also a civil law scheme set out in Part 6 of the *Online Safety Act 2015* (Cth), which creates civil penalty offences for posting intimate images on social media without a person's consent.

[1134] See Attorney-General's Department (Cth), *National Statement of Principles Relating to the Criminalisation of the Non-Consensual Sharing of Intimate Images* (2017) <https://www.ag.gov.au/crime/publications/national-statement-principles-relating-criminalisation-non-consensual-sharing-intimate-images>.
[1135] See Asher Flynn, Jonathan Clough and Talani Cooke, 'Disrupting and Preventing Deepfake Abuse; Exploring Criminal Law Responses to AI-Facilitated Abuse' in Anastasia Powell, Asher Flynn and Lida Sugiura (eds), *The Palgrave Handbook of Gendered Violence and Technology* (Palgrave Macmillan, 2021) 583.
[1136] See Clare McGlynn, Kelly Johnson and Anastasia Powell, '"It's Torture for the Soul": The Harms of Image-Based Sexual Abuse' (2021) 30 *Social and Legal Issues* 541. See also Joanne Worsley and Grace carter, 'The Impact of Technology-Facilitated Sexual Violence: A Literature Review of Qualitative Research' in Anastasia Powell, Asher Flynn and Lida Sugiura (eds), *The Palgrave Handbook of Gendered Violence and Technology* (Palgrave Macmillan, 2021) 261.
[1137] Clare McGlynn, Kelly Johnson and Anastasia Powell, '"It's Torture for the Soul': The Harms of Image-Based Sexual Abuse' 543 quoting Clare McGlynn and Erika Rackley, *Image-Based Sexual Abuse* (2017) 37 *Oxford Journal of Legal Studies* 535, 546.
[1138] See discussion at [10.2].
[1139] See [10.12.4].
[1140] Parliament of Tasmania, 'Civil Digital Communications Bill 2017' (Web Page, 2021) <https://www.parliament.tas.gov.au/Bills/Bills2017/62_of_2017.html>.
[1141] *Criminal Code Act 1995* (Cth) vol 2 sch, s 474.17A.

The penalties can be imposed by a Federal Court or the Federal Circuit Court, following application by the National e-Safety Commissioner. The National e-Safety Commissioner also gained various powers under the amendments, including powers to investigate complaints with respect to intimate images, issue infringement notices, and require social media providers to take reasonable steps to remove intimate images. As with the amendments to the federal criminal law, this is largely targeted at image-based abuse.

10.12.6 These provisions were retained and largely replicated in the *Online Safety Act 2021* (Cth). This Act further introduced a complaints-based removal notice system and further strengthened the e-Safety Commissioner's powers to allow for ordering the removal of material posted with the likely intention of causing serious harm, including cyberbullying and image-based abuse.[1142] This Act is intended to operate concurrently with State and Territory laws.[1143]

10.12.7 In 2017, Commonwealth, State, and Territory jurisdictions agreed to the *National Statement of Principles Relating to the Criminalisation of the Non-Consensual Sharing of Intimate Images*.[1144] This led to nearly all States and Territories passing laws that introduced offences concerning the distribution of intimate images and offences to threaten to send an intimate image without consent. For example, the *Crimes Act 1900* (NSW) Section 91Q creates an offence of distributing an intimate image without consent, and Section 91R creates an offence of threatening to record or distribute an intimate image. Similar offences have also been introduced in Queensland, the ACT, Victoria, Western Australia, the Northern Territory, and South Australia.[1145] Notably, Tasmania remains the current exception where such crimes have *not* been introduced. In the creation of such an offence, the law should make it clear that the prohibition extends to distributing (or threatening to distribute) images created or modified by the use of artificial intelligence.[1146]

10.13 The Commonwealth Privacy Act Review

10.13.1 The Commonwealth Privacy Act Review considered ways to protect privacy as alternatives or in addition to the creation of statutory tort. One option considered was the extension of the protections under the Privacy Act to individuals to provide greater options for a victim, including making a complaint or applying to the courts under a direct right of action, rather than to litigate a tort. However, this option was not the Review's preferred approach, given the regulation of intimate image abuse was already provided for in the *Online Safety Act 2021* (Cth). However, the Review stated that '[i]t may be appropriate to consider the feasibility of a mechanism to enable individuals to seek compensation against perpetrators as part of the eSafety framework to achieve a less fragmented approach'.[1147]

[1142] Supplementary Explanatory Memorandum, Online Safety Bill 2021 (Cth) 1.
[1143] *Online Safety Act 2021* (Cth) s 234.
[1144] Attorney-General's Department (Cth), *National Statement of Principles Relating to the Criminalisation of the Non-Consensual Sharing of Intimate Images* (2017) <https://www.ag.gov.au/crime/publications/national-statement-principles-relating-criminalisation-non-consensual-sharing-intimate-images>.
[1145] See *Summary Offences Act 1966* (Vic) ss 40, 41A, 41B, 41C, 41DA, 41DB; *Crimes Act 1958* (Vic) Div 1 pt (8FAAB); *Criminal Code* (WA) ss 221BA–22BF, 338, 338B, 338C; *Crimes Act 1900* (ACT) Div 15C; *Criminal Code 1983* (NT) Part VI, Div 7A; *Criminal Code 1899* (Qld) s 207A, 223, 229A; *Summary Offences Act 1953* (SA) ss 26A–26E; *Crimes Act 1900* (NSW) Div 15C, ss 91N, 91Q, 91R.
[1146] For example, the *Crimes Act 1900* (NSW) s 91N defined 'intimate image' to mean 'an image of a person's private parts, or of a person engaged in a private act, in circumstances in which a reasonable person would reasonably expect to be afforded privacy, or an image that has been altered to appear to show a person's private parts, or a person engaged in a private act, in circumstances in which a reasonable peons would reasonably expect to be afforded privacy'.
[1147] Privacy Act Review Report 2022 27.3.2.

10.14 Consultation

10.14.1 The TLRI Issues Paper invited submissions on privacy in the context of the unauthorised sharing of intimate images in response to the following question:

> Are the existing legislative protections (largely at the Commonwealth level) against image-based abuse and similar online privacy interferences adequate to protect individual privacy, or should the Tasmanian Parliament enact new criminal offences or civil remedies for such egregious online interferences with privacy, as other Australian jurisdictions have done? [1148]

10.14.2 Three submissions addressed this question; all considered that the law should be updated.[1149] Meg Webb MLC considered that new criminal offences should be created in Tasmania, or at least civil remedies, for image-based abuse and similar online privacy interferences, consistent with other Australian jurisdictions. Similarly, Youth Law Australia highlighted that Tasmania had not introduced specific offences concerning distribution of intimate images without consent and is the only jurisdiction not to have done so. Youth Law Australia stressed that the sharing of intimate images is not only a privacy concern, but also a harmful form of sexual violence, having potentially devastating consequences.

10.14.3 In its submission, Youth Law Australia also commented on the particular vulnerability of children and young people and that there was often little a victim can do to negate damage (especially if the image is shared on internet and social media). Youth Law Australia submitted that Tasmania should have specific offences that:

- clearly apply to threatened and actual sharing of intimate images without consent to reflect the gravity of this conduct and to bring Tasmania into line with other states and territories; and
- make it clear that young people below a certain age (for example, 16) cannot consent to sharing of an intimate image that involves them.

10.15 The TLRI's view

10.15.1 As recognised by Youth Law Australia, and in research literature, the unauthorised sharing of intimate images can cause considerable harm. While the Commonwealth *Criminal Code* creates an offence where it is done through the use of a carriage service (which would apply to online sharing) and there is a federal civil image-based abuse scheme, it is the TLRI's view that Tasmania should, in line with other jurisdictions, enact state-based legislation to creating offences of distributing an intimate image without consent or threatening to distribute an intimate image. This is consistent with the *National Statement of Principles relating to the Criminalisation of the Non-consensual Sharing of Intimate Image*, which set out principles for nationally consistent criminal offences.

[1148] Issues Paper Part 4, Question 4.6
[1149] Submission 3 (Anonymous); Submission 8 (Meg Webb MLC); Submission 12 (Youth Law Australia).

10.16 Recommendation

Recommendation 61: Tasmania should, in line with other jurisdictions, enact state-based legislation to create offences of distributing an intimate image without consent or threatening of distribute an intimate image. In the creation of such an offence, the law should make it clear that the prohibition extends to distributing (or threating to distribute) images created or modified by the use of artificial intelligence.

10.17 Additional protections of health information

The Tasmanian position

10.17.1 The *Health Complaints Act 1995* (Tas) ('Health Complaints Act') provides for the making, investigation, conciliation, and reference of complaints against public and private health services.

10.17.2 For the purposes of that Act, 'health service'[1150] is broadly defined to mean a service provided to a person for, or purportedly for, the benefit of human health, encompassing both services provided at certain places, such as hospitals or nursing homes, and services provided by various listed health professionals.[1151] They include:

- medical, dental, pharmaceutical, or mental health services;
- aged care or disability care;
- natural or alternative health care;
- laboratory and other support services;
- the provision of information relating to promoting health care or health education; and
- any other service for the care or treatment of another person.

10.17.3 The Health Complaints Act empowers the Governor of Tasmania to appoint a Health Complaints Commissioner ('HCC'), whose functions include: receiving, assessing, and resolving complaints; identifying and reviewing issues arising out of complaints; and suggesting ways to improve health services and preserve and increase health rights; preparing and regularly reviewing a Charter of Health Rights; and providing information, education, and advice, among other things.[1152] Mr Richard Connock was appointed as the Tasmanian Ombudsman and HCC in July 2014.[1153]

10.17.4 Complaints to the HCC may be made by health service users, by representatives or parents/guardians of children, and by people holding powers of attorney for a health service user, among others. Complaints can be made about a wide range of matters, including that 'a health service provided

[1150] This can be compared to the definition of 'health service' in the PIPA, see above at (n 235).
[1151] *Health Complaints Act 1995* (Tas) sch 1 pt 1. Note that services related to claims under the *Workers Rehabilitation and Compensation Act 1988* (Tas) and action under the *Asbestos-Related Diseases (Occupational Exposure) Compensation Act 2011* (Tas) are not health services: ibid sch 1 pt 2.
[1152] *Health Complaints Act 1995* (Tas) ss 5, 6.
[1153] Health Complaints Commissioner Tasmania, *About Us* (Web Page) <https://www.healthcomplaints.tas.gov.au/about-us>.

failed to respect a health service user's privacy or dignity'[1154] and that 'a health service provider acted unreasonably in disclosing information in relation to a health service user'.[1155]

10.17.5 Compliance with the *Tasmanian Charter of Health Rights and Responsibilities* ('the Charter'), created by the HCC, is one of the grounds for complaint under the Health Services Act.[1156] The Charter must be taken into account when assessing whether a health service's actions were reasonable.[1157] Some rights listed in the Charter relate to information confidentiality, privacy, and security. These include the right to have personal health information and any sensitive matters kept confidential, including that '[n]o identifying information about the consumer, his/her condition or treatment may be disclosed without his/her consent unless the disclosure is required or authorised by law', and the right to expect that information about one's health is 'kept securely and cannot be easily accessed by unauthorised persons'.[1158]

10.17.6 The HCC must assess complaints made under the Health Complaints Act within 45 days, and either: (1) refer the complaint to an appropriate body, such as the Ombudsman or a relevant professional registration board; (2) refer the complaint for conciliation; (3) investigate the complaint; or (4) dismiss the complaint.[1159] The HCC also has the power to investigate matters referred by the Health Minister or on the HCC's own initiative.

10.17.7 The Health Complaints Act facilities the making and investigating of complaints in several respects. For example, it overrides legislation that hinders the disclosure or communication of information, if such hindrance would prevent or restrict the making of a complaint or the conduct of an investigation under the Act.[1160]

10.17.8 The Health Complaints Act also confers extensive investigation powers on the HCC, including the power to compel provision of documents,[1161] examine witnesses,[1162] apply for the issue of a warrant,[1163] and enter any premises occupied or used by a health service or health service provider.[1164] Further, it obliges secrecy on the part of those who administer the Act by imposing extensive obligations of confidentiality regarding information and actions taken under the Act.[1165] However, if a recording, disclosure, or use of statistical or other information could not reasonably be expected to lead to the identification of any person, it is not limited under the Act.[1166]

10.17.9 If the HCC investigates a complaint and forms the view that the complaint is justified, but the complaint appears incapable of being resolved, the HCC can provide a 'notice of recommended action' to the health provider which sets out the particulars of the complaint, the reasons for the decision, and any action the HCC considers the provider ought to take to remedy each unresolved grievance raised in

[1154] *Health Complaints Act 1995* (Tas) s 23(1)(f).
[1155] *Health Complaints Act 1995* (Tas) s 23(1)(i).
[1156] Ibid s 23(1)(k).
[1157] Ibid s 75.
[1158] *Tasmanian Charter of Health Rights and Responsibilities* arts 1, 3.
[1159] *Health Complaints Act 1995* (Tas) s 25.
[1160] *Health Complaints Act 1995* (Tas) s 62B.
[1161] *Health Complaints Act 1995* (Tas) s 45.
[1162] *Health Complaints Act 1995* (Tas) s 46.
[1163] *Health Complaints Act 1995* (Tas) s 47.
[1164] *Health Complaints Act 1995* (Tas) s 47A.
[1165] *Health Complaints Act 1995* (Tas) s 65. These include penalties for recording, disclosing, or using confidential information gained through administration of the Act unless it is necessary for the purposes of the Act, expressly authorised or required under other legislation or regulations, or authorised in writing by the person to whom it relates.
[1166] *Health Complaints Act 1995* (Tas) s 65(5).

the complaint.[1167] The provider must respond in writing within 45 days, advising the HCC of action taken to remedy the grievances.[1168] Failure to comply with this requirement is subject to penalty of a fine not exceeding 50 penalty points.[1169]

10.17.10 Other Tasmanian legislation touches on other forms of privacy in the health context. For example, the *Forensic Procedures Act 2000* (Tas) provides for privacy protection in relation to forensic procedures relating to offences, including the taking of medical samples or the conduct of bodily examinations. Forensic procedures, including taking a saliva or DNA swab of a young person, must be carried out in a way that affords 'reasonable privacy' to the person undergoing the procedure.[1170]

The position in other jurisdictions

10.17.11 Other States and Territories have similar legislation that enables health service users to make complaints about health practitioners and health services, including complaints relating to privacy, and establishes a body to handle and take action in relation to complaints. These include the NSW Health Care Complaints Commissioner,[1171] the Queensland Office of the Health Ombudsman,[1172] the Victorian Health Complaints Commission,[1173] and the Western Australian Health and Disability Services Complaints Office.[1174]

10.18 Consultation

10.18.1 The TLRI Issues Paper did not pose any questions about privacy protections of health information outside the PIPA.

10.19 The TLRI's view

10.19.1 The TLRI's view is that there is a need for harmonisation of legislation and standards to allow for safe and consistent sharing of health information in line with the Australian Digital Health Agency's *National Health Interoperability Plan*. There are several options for achieving this in Tasmania, including amending the PIPA to align with the Privacy Act, establishing a Health Information Privacy Code via amendment to the PIPA,[1175] or creating dedicated Health Information Legislation similar to that found in some other jurisdictions, such as Victoria.

10.19.2 Accordingly, the TLRI's view is that there should be further consideration of necessary reforms to the PIPA, or the creation of standalone legislation, to align Tasmanian regulation with the *National Health Interoperability Plan*.

[1167] *Health Complaints Act 1995* (Tas) s 56(1), (2)
[1168] *Health Complaints Act 1995* (Tas) s 56(3).
[1169] *Health Complaints Act 1995* (Tas) s 56(3).
[1170] *Forensic Procedures Act 2000* (Tas) ss 34K(1)(b), 35(a).
[1171] *Health Care Complaints Act 1993* (NSW) s 76.
[1172] *Health Ombudsman Act 2013* (Qld) s 24.
[1173] *Health Complaints Act 2016* (Vic) s 110.
[1174] *Health and Disability Services (Complaints) Act* 1995 (WA).
[1175] The potential value of privacy codes is discussed in Part 8 of this Report.

10.20 Recommendation

Recommendation 62: There should be further consideration of necessary reforms to the PIPA, or the creation of standalone legislation, to align Tasmanian regulation with the *National Health Interoperability Plan*.

Part 11

General Law Protections and a Civil Statutory Cause of Action

11.1 Introduction

11.1.1 As discussed at [2.5.23] and following of this Final Report, few Australian courts (and even fewer in Tasmania) have dealt with cases concerning interference with privacy. The Supreme Court of Tasmania has made comments about privacy protection in a number of cases, including cases involving the relevance of privacy to the administration of justice, cases involving the application of legislation that identifies privacy as a factor to be taken into account by a decision-maker, and cases where a party has invoked international instruments that establish a right to privacy.[1176]

11.1.2 In some cases of egregious interferences with privacy, appellate courts in the Commonwealth and other State and Territory jurisdictions have provided equitable remedies, such as finding that the interference was a breach of confidence and awarding damages in compensation.[1177] The High Court of Australia, in the 2001 case of *Lenah Game Meats*,[1178] left open the possibility that a common law cause of action for breach of privacy will be established. Two lower courts (in Victoria and Queensland) subsequently recognised a tort of invasion of privacy,[1179] but the common law has not further developed since that time. Recent Commonwealth and State inquiries have recognised the absence of a standalone privacy right or civil remedy that comprehensively covers privacy interferences as a significant gap in individuals' privacy protections and have recommended the introduction of statutory causes of action to fill this gap.[1180]

11.1.3 This Part discusses the development of the common law in Australia relating to a potential tort of interference with privacy and arguments in favour of (and against) the introduction of a statutory tort of privacy at either the State or Commonwealth level.

11.2 The current position at common law

11.2.1 No appellate court in Australia, and no Tasmanian court, has recognised a tort of interference with privacy, whether this includes information privacy, physical privacy, or both. Nor has any such court granted remedies in tort law for interferences with privacy.

[1176] For example, *R v Brown* [2014] TASSC 18; *R v Pettit* [2015] TASSC 14; *Tasmania v Wykes* [2019] TASSC 18; *Carnevale v Baker* [1996] TASSC 9 [20]; *Tasmania v Melick* [2019] TASSC 19 [13], [20](d); *Sierra 4 v Moles* [1994] TASSC 38.
[1177] *Giller v Procopets [No 2]* (2008) 24 VR 1; *Wilson v Ferguson* [2015] WASC 15.
[1178] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 ('*Lenah Game Meats*').
[1179] *Grosse v Purvis* [2003] QDC 151; *Doe v Australian Broadcasting Corporation* [2007] VCC 281.
[1180] See [11.3.5] below.

11.2.2 The 2001 High Court case, *Lenah Game Meats*,[1181] raised the possibility of a standalone action for interference with individual privacy to be recognised by Australian courts when the appropriate facts arise, although the majority held that it was not an appropriate case to find whether a tort of privacy should exist.[1182] In *Lenah Game Meats*, each of the five judges recognised the normative importance of privacy and its protection and acknowledged that Australian law is sufficiently capacious to accommodate protection for privacy. None of the justices excluded tort law as the vehicle for this protection.

11.2.3 The High Court in *Lenah Game Meats* also suggested that common law privacy protection was not necessarily excluded by the 1937 case of *Victoria Park Racing*, which is often cited as authority for the rejection of a right to privacy.[1183] In the case of *Smethurst v AFP*, the High Court indicated it was open to the possibility of recognising a tort of interference with privacy and grant tortious remedies, including compensation for harm suffered.[1184]

11.2.4 Since *Lenah Game Meats*, there has been inconsistency among lower courts in their willingness to grant remedies for interferences with privacy. Some have done so, including by granting damages under a tort of invasion of privacy.[1185] Others have refused to recognise any such action, whether as a tort or otherwise, even where the plaintiff is an individual rather than a corporation.[1186]

11.2.5 Appellate courts have twice considered whether to grant a remedy for interference with privacy, either as a tort or as another form of civil action. In both cases, the court did not use the door left open in *Lenah Game Meats* to recognise a tort of interference with privacy. Instead, the court granted compensation under the equitable action of breach of confidence.[1187]

11.2.6 The first was *Giller v Procopets* in the Victorian Court of Appeal, where the plaintiff's former partner (the defendant) published sexual information about the plaintiff. The Court recognised that the harm was the plaintiff's distress caused by the interference with her privacy. While holding that this harm could ground an action for damages, the Court limited the action to breach of confidence in equity and declined to recognise a tort of interference with privacy. Subsequently, the Supreme Court of Western Australia in *Wilson v Ferguson* endorsed this approach to fashioning of equitable remedies for gross breach of privacy.[1188]

11.2.7 Given that *Lenah Game Meats* presents an open door to recognising tortious liability for interference with privacy, it is unclear whether compensatory damages in equity are appropriate for non-tortious harm to dignity or distress (the harm recognised as actionable in *Giller v Procopets*).[1189]

[1181] *Lenah Game Meats*.
[1182] See Jelena Gligorijevic, 'A Common Law Tort of Interference with Privacy for Australia: Reaffirming *ABC v Lenah Game Meats*' (2021) 44(2) *University of New South Wales Law Journal* 673, 686–7 ('Reaffirming *ABC v Lenah Game Meats*').
[1183] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479; see, eg, *Lenah Game Meats* (n 1181) [185]–[189].
[1184] *Smethurst v Commissioner of the Australian Federal Police* (2020) 94 ALJR 502, [48], [86], [129].
[1185] *Grosse v Purvis* [2003] QDC 151; *Doe v Australian Broadcasting Corporation* [2007] VCC 281.
[1186] *Kalaba v Commonwealth of Australia* [2004] FCA 763. It was also noted by Callinan J in *Batistatos v Roads & Traffic Authority of New South Wales* (2006) 226 CLR 256, that, following *Lenah Game Meats*, some courts' refusal to recognise an actionable privacy claim means Australian common law is not yet ready to entertain standalone privacy claims: at [216].
[1187] *Giller v Procopets [No 2]* (2008) 24 VR 1; *Wilson v Ferguson* [2015] WASC 15.
[1188] *Wilson v Ferguson* [2015] WASC 15.
[1189] See Gligorijevic, 'Reaffirming *ABC v Lenah Game Meats*'; J D Heydon, M J Leeming and P G Turner, *Meagher, Gummow and Lehane's Equity: Doctrines and Remedies* (LexisNexis Butterworths, 5th ed, 2015)

11.3 A civil cause of action for interference with privacy

The position in Tasmania

11.3.1 Since the High Court decision in *Lenah Game Meats*, the Supreme Court of Tasmania has not had an opportunity to adjudicate a claim seeking tortious or other remedies for interference with privacy. Consequently, there is currently no civil cause of action (and therefore no remedy) in Tasmania that covers interferences with privacy in a comprehensive manner. Instead, as outlined elsewhere in this Report, there are various sources of privacy protection and remedies for breaches of those protections, including under the *Personal Information Protection Act 2004* (Tas) ('PIPA'), which address some types of privacy in some contexts.

11.3.2 The piecemeal nature of existing protections means there is a range of circumstances in which a person may suffer a serious invasion of their privacy but have no legal avenue through which to seek compensation or another civil remedy.

11.3.3 One of these gaps—the unavailability of compensation or other orders for breaches of the PIPA—is discussed in Part 8 of this Report.

11.3.4 Even if that gap is addressed through the proposed reform, other circumstances that are addressed to some extent in other Tasmanian legislation would still not give rise to a cause of action for invasion of privacy. As set out in the Issues Paper, these include:

- misuse of private information by non-governmental actors, including the media, journalists, advertising corporations, and data processing entities;[1190]
- image-based abuse and other non-consensual acquisition and use of intimate images, including where the individual in the image is not identifiable by the public at large;[1191]
- use of private information for the purposes of blackmail;[1192]

882–883; P G Turner, 'Privacy Remedies Viewed through an Equitable Lens' in Jason N E Varuhas and N A Moreham (eds), *Remedies for Breach of Privacy* (Hart Publishing, 2018) 265.

[1190] The development of common law privacy protection in jurisdictions outside Australia has largely been based on media intrusions: see, eg, *Campbell v MGN Ltd* [2004] 2 AC 457; *PJS v News Group Newspapers Ltd* [2016] AC 1081; *Hosking v Runting* [2005] 1 NZLR 1. However, it is noted here and with regard to (n 1198) that cases in the jurisdiction of the United Kingdom must be seen against the backdrop of the *Human Rights Act 1998* (UK), which implements relevant provisions of the European Court of Human Rights. Case law in the United Kingdom uses the language of a 'reasonable expectation of privacy', most recently being described as a tort of misuse of private information: see, eg, *ZXC v Bloomberg LP* [2022] 2 WLR 424. For the Council of Europe jurisdiction and the human right to a private and family life, see *Von Hannover v Germany (No 1)* [2004] EMLR 21.

[1191] Such situations have resulted in equitable remedies in breach of confidence in some Australian courts: see, eg, *Giller v Procopets (No 2)* (2008) 24 VR 1; cf *Wilson v Ferguson* [2015] WASC 15. For a critical discussion of why equitable remedies are inappropriate for this type of harm, see Gligorijevic, 'Reaffirming *ABC v Lenah Game Meats*'; and Turner, 'Privacy Remedies Viewed through an Equitable Lens' 265. For an example of where a sexual photograph of an unidentifiable individual was made public and led to a remedy when litigated: see *L v G* [2002] DCR 234 (District Court of New Zealand). Judge Abbott reasoned that there was sufficient dignitary harm and humiliation in the fact that the plaintiff could identify herself from the photograph, and that that was sufficient to ground a remedy in tort law.

[1192] Interim injunction applications in response to privacy blackmail threats are common in England and Wales. See, eg, *AMM v HXW* [2010] EWHC 2457 (QB); *KJH v HGF* [2010] EWHC 3064 (QB); *LJY v Persons Unknown* [2018] EMLR 9; *AXB v BXA* [2018] EWHC 588 (QB).

- aggressive media reportage activities, including 'door-stepping' and 'grief journalism';[1193]
- online sharing or publication of a child's image or information by that child's parent or guardian, referred to as 'sharenting', and where this creates a digital dossier for that child;[1194]
- interferences with the privacy of third parties involved in or affected by law enforcement investigations or judicial processes (for example, victims of an offence, family members, or relatives of an accused, and children of parties to divorce proceedings);[1195]
- intrusions upon the privacy of public figures, such as voluntary public figures (for example, celebrities and politicians) and involuntary public figures (for example, the children of voluntary public figures), including where the public figure has revealed some aspects of their private life, but wishes to keep other aspects private;[1196]
- 'kiss and tell' stories, involving one party to a private or intimate relationship wishing to sell or disclose private or intimate information which also relates to the other party or parties to that relationship, where the latter party or parties do not consent or are opposed to that disclosure;[1197]
- intrusions upon privacy, including taking targeted photographs or recordings of individuals engaging in anodyne activities and/or in a public space (for example, a family outing to a restaurant, where there is no consent to publication of the activity to the world at large, and especially when photos are taken of a child, who in some cases may have a reasonable expectation of privacy where an adult does not);[1198]
- use of Remotely Piloted Aircraft ('RPA') or Unmanned Aerial Vehicles ('UAV') (drones) in a way that is intended to have, or in fact has,[1199] and
- general intrusions upon seclusion, whether or not they involve audio-visual recording.[1200]

[1193] For an instance of media misuse of private information in such circumstances in England, see *Richard v British Broadcasting Corporation* [2019] ch 169. See also NA Moreham and Y Tinsley, 'Media Intrusion into Grief: Lessons from the Pike River Mining Disaster' in AT Kenyon (ed), *Comparative Defamation and Privacy Law* (Cambridge University Press, 2016) 115.

[1194] See Jelena Gligorijevic, 'Children's Privacy: The Role of Parental Control and Consent' (2019) 19(2) *Human Rights Law Review* 201.

[1195] For a summary of how the courts in England and Wales have addressed the conflict between privacy and open justice (and freedom of expression) in processes and publications associated with the administration of justice, see Jelena Gligorijevic, 'Publication Restrictions on Judgements and Judicial Proceedings: Problems with the Presumptive Equivalence of Rights' (2017) 9(2) *Journal of Media Law* 215.

[1196] For a summary of the public figure doctrine in English and Welsh privacy law and European human rights law: see Kirsty Hughes, 'The Public Figure Doctrine and the Right to Privacy' (2019) 78(1) *Cambridge Law Journal* 70.

[1197] Such actions have resulted in privacy injunctions (at least interim injunctions) in the English and Welsh jurisdiction: see, eg, *CTB v NGN Ltd* [2011] EWHC 1326 (QB); *PJS v News Group Newspapers Ltd* [2016] AC 1081. However, some such applications have also failed: see, eg, *Theakston v MGN Ltd* [2002] EMLR 22; *YXB v TNO* [2015] EWHC 826 (QB). Other such cases resulted in anonymity orders, requiring any publication of the relevant information not to reveal the identity of the other party: see, eg, *NEJ v BDZ* [2011] EWHC 1972 (QB); *MJN v NGN Ltd* [2011] EWHC 1192 (QB).

[1198] See, eg, *Murray v Big Pictures Ltd* [2008] 3 WLR 1360; *Weller v Associated Newspapers Ltd* [2016] 1 WLR 1541.

[1199] See [10.2.18]–[10.2.19] for discussion of the regulation on the use of drones in Australia from a privacy perspective.

[1200] See, eg, *C v Holland* [2012] 3 NZLR 672 (High Court of New Zealand). See also N A Moreham, 'Beyond Information: Physical Privacy in English Law' (2014) 73(2) *Cambridge Law Journal* 350; P Wragg, 'Recognising a Privacy-Invasion Tort: The Conceptual Unity of Informational and Intrusion Claims' (2019) 78(2) *Cambridge Law Journal* 409. See [10.2] for discussion of criminal liability for unlawful surveillance.

The position in other jurisdictions

11.3.5 Multiple inquiries in recent years have recommended that a statutory cause of action for serious invasions of privacy be created either at State or Commonwealth level. This is consistent with calls from legal scholars who have engaged with the prospect of a civil remedy for interference with privacy with a view to, among other things, addressing gaps where protection is lacking—particularly in relation to physical privacy of the person.[1201]

11.3.6 At the State level, the NSW Law Reform Commission,[1202] the NSW Standing Committee on Law and Justice,[1203] the Victorian Law Reform Commission,[1204] the South Australian Law Reform Institute,[1205] and the Queensland Crime and Corruption Commission[1206] have all recommended the enactment of statutory civil causes of action for serious invasion of privacy. No such legislation has yet been enacted in these jurisdictions.[1207]

11.3.7 At the Commonwealth level, the Australian Law Reform Commission's ('ALRC') *For Your Information Final Report* (Report 108) recommended the introduction of a statutory cause of action for serious invasions of privacy in 2008, on the basis that relying on developments in the common law could result in 'piecemeal and fragmented privacy protection' and consequent uncertainty for individuals and organisations.[1208]

11.3.8 The ALRC was subsequently asked to design such a statutory cause of action, which was published in its 2014 report, *Serious Invasions of Privacy in the Digital Era*.[1209] The ALRC recommended that a cause of action be enacted by the Commonwealth in a standalone Act, on the basis that this would be 'the best way to ensure the action is available and consistent throughout Australia' and would avoid confusion, fragmentation, and complexity that may arise if multiple States and Territories enacted their own provisions.[1210]

11.3.9 The ALRC recommended that the cause of action be described in the Act as an action in tort for several reasons, including that it would:

[1201] See, eg, David Lindsay, 'Protection of Privacy under the General Law Following *ABC v Lenah Game Meats*: Where to Now' (2002) 9(6) *Privacy Law and Policy Reporter* 101; Des Butler, 'A Tort of Invasion of Privacy in Australia?' (2005) 29(2) *Melbourne University Law Review* 339; Michael Tilbury, 'Privacy: Common Law or Human Right?' in Normann Witzleb et al (eds), *Emerging Challenges in Privacy Law: Comparative Perspectives* (Cambridge University Press, 2014) 157; Gligorijevic, Reaffirming *ABC v Lenah Game Meats*'.
[1202] New South Wales Law Reform Commission, *Invasion of Privacy* (Report 120, April 2009) 4.
[1203] Standing Committee on Law and Justice, *Inquiry into Remedies for the Serious Invasion of Privacy in New South Wales* (Final Report, Parliament of New South Wales, March 2016) Recommendation 3.
[1204] Victorian Law Reform Commission, *Surveillance in Public Places* (Final Report 18, May 2010) Recommendations 22–26.
[1205] South Australian Law Reform Institute, *A Statutory Tort for Invasion of Privacy* (Final Report 4, March 2016) Recommendation 1.
[1206] Crime and Corruption Commission Queensland, *Operation Impala: Report on Misuse of Confidential Information in the Queensland Public Sector* (February 2020) Recommendation 17.
[1207] The *Civil Liability (Serious Invasions of Privacy) Bill 2021* (SA) was tabled in South Australian Parliament and circulated for comment in 2021 but has not been progressed as at the date of finalisation of this report.
[1208] ALRC, *Privacy* 2535–2536 ([74.1]–[74.2]).
[1209] ALRC, *Serious Invasions of Privacy in the Digital Era* 18.
[1210] Ibid 59–60.

- provide certainty about 'a number of ancillary issues that will inevitably arise' for courts (for example, many existing legislative provisions refer to liability in tort and describing the privacy action as a tort action would integrate it into existing laws);[1211]
- be consistent with accepted legal classifications;
- be consistent with nomenclature in international jurisdictions, thus enabling Australian courts to benefit from international case law;
- distinguish the cause of action from existing regulatory regimes, such as the Privacy Act; and
- differentiate this cause of action from the equitable and contractual actions for breach of confidence, which would continue to exist.[1212]

11.3.10 Under the ALRC model, the tort would be available in the following circumstances:[1213]

- where the invasion of privacy was either an intrusion into seclusion or a misuse of private information;
- where it is proved that a person in the position of the plaintiff would have had a reasonable expectation of privacy in all the circumstances;
- where the invasion was committed intentionally or recklessly (with mere negligence being insufficient);
- where the invasion was 'serious'
- regardless of whether the invasion has caused 'actual damage' (that is, 'the wrong itself is the harm',[1214] and damage may include emotional distress);
- where the court is satisfied that the public interest in privacy outweighs any countervailing public interests (that is, it is subject to a 'balancing exercise' where the court must consider privacy against other public interests, including freedom of speech, freedom of the media, public health and safety, and national security).

11.3.11 The ALRC recommended that a range of defences be available, including:[1215]

- a defence of lawful authority (where conduct was required or authorised by law);
- a defence where the conduct was incidental to defence of persons or property;
- a defence of necessity (where a defendant acts in a reasonable belief they were preventing imminent and greater harm);
- a defence of consent (including express and implied consent);
- a defence of absolute privilege (where information is revealed in the course of public fora, such as in parliament or in court or tribunal proceedings);[1216]
- a defence for the publication of public documents; and
- a defence for fair reporting of public proceedings.

[1211] ALRC, *Serious Invasions of Privacy in the Digital Era* 69.
[1212] Ibid 67–70.
[1213] Ibid 19, chs 5–9.
[1214] Ibid 138.
[1215] Ibid 185–186, ch 11.
[1216] ALRC, *Serious Invasions of Privacy in the Digital Era* 202.

11.3.12 Finally, the ALRC proposed that a range of orders remedies be available for serious invasions of privacy, including: damages; an account of profits; injunctions; delivery up, destruction, and removal of material; correction and apology orders; and declarations.[1217]

11.3.13 The ALRC expressed the view that the introduction of a statutory cause of action in this form would be within the scope of the Commonwealth's constitutional powers and would not infringe on the implied limitation on the Commonwealth's power to legislate to burden the exercise of powers and functions of the States.[1218]

11.3.14 The implementation of the ALRC's proposed model has since been recommended by other Commonwealth inquiries, including the ACCC's *DPI Report*[1219] and the AHRC's *Human Rights and Technology Final Report*.[1220]

11.3.15 The Australian Competition and Consumer Commission ('ACCC') argued that a statutory cause of action would 'lessen the bargaining power imbalance between consumers and digital platforms by providing Australian consumers with an additional way of seeking redress or poor data practices by digital platforms and other businesses that collect Australians' personal information'.[1221]

11.3.16 The Australian Human Rights Commission ('AHRC') noted that such a reform would 'present a barrier to intrusive, wide-scale surveillance' and 'extend privacy protection in Australian law beyond personal information, to include interference with bodily and territorial privacy' in a manner more appropriate to implementing Australia's obligations under Article 17 of the *International Convention on Civil and Political Rights* ('ICCPR') (discussed at [2.4]).[1222]

11.4 The Commonwealth Privacy Act Review

11.4.1 The Commonwealth Privacy Act Review also supported the implementation of the ALRC's model of a statutory tort for serious invasions of privacy.[1223]

11.4.2 The Review reiterated that a statutory cause of action is warranted due to the lack of protection of a range of invasions of privacy in the *Privacy Act*, citing the Office of the Australian Information Commissioner's ('OAIC') list of circumstances not currently covered by the Act:

- 'peering over a back fence to take a video of someone in their backyard, or other place where there is an expectation of privacy (for example, in a public bathroom)';
- 'recording a private conversation with someone without their knowledge or consent';
- 'interfering with, misusing or disclosing an individual's private correspondence or private written, oral or electronic communication';
- 'disclosing or disseminating sensitive facts relating to an individual's private life';

[1217] Ibid 20, ch 12.
[1218] Ibid 67.
[1219] ACCC, *DPI Inquiry Report* Recommendation 19.
[1220] AHRC, *Human Rights and Technology Final Report* (2021) Recommendation 21.
[1221] ACCC, *DPI Inquiry Report* 493.
[1222] AHRC, *Human Rights and Technology Final Report* 123.
[1223] Privacy Act Review Report 2022 Proposal 27.1.

- 'misusing personal information about another person that was accessed in breach of an employment contract, but for which the employer is not liable because it was misused for a personal purpose (for example, blackmail or Family Court proceedings)'; and
- 'a data breach experienced by a small business or individual not covered by the Act'.[1224]

11.4.3 The Review agreed with the ALRC's conclusion that it would be most appropriate for a statutory tort to be enacted in a standalone Commonwealth Act (not the Privacy Act), so that it applied throughout Australia, and not only to Australian Privacy Principles ('APP') entities and Commonwealth agencies, but also State and Territory agencies and individuals.[1225]

11.4.4 The Review emphasised that consultation with the States and Territories was essential to ensure that the approach was consistent nationwide, especially in light of the recommendations for the introduction of State-level statutory torts already made in South Australia, NSW, and Queensland (see [11.3.6] and following) and in order to ensure that:

- State agencies have the necessary lawful authorisations for activities that may be covered by the tort; and
- State and Territory courts are adequately resourced to deal with any potential impacts of the introduction of the tort.[1226]

11.4.5 The Commonwealth Government agreed in-principle that a statutory tort based on the ALRC's model should be introduced. It stated that further consultation should be undertaken with media organisations in light of concerns about impacts on public interest journalism, as should further consultation with States and Territories on potential implications for State and Territory courts and agencies.[1227]

11.5 Consultation

11.5.1 The TLRI Issues Paper invited submissions in response to the following questions:

> Does existing judicial recognition of privacy (either through equitable remedies or as a nascent constitutional principle) provide adequate protection for individual privacy, especially in circumstances not covered by the PIPA and other legislative protections?[1228]
>
> Should the Tasmanian Parliament legislate to introduce a statutory civil cause of action for interference with privacy in Tasmania in place of or in addition to existing legal protections? If so, how should this cause of action be framed, taking into account the matters of threshold and scope, breach, defences, and remedies?[1229]

11.5.2 Two submissions responded to the first of these questions: 'Maybe',[1230] and 'No, not necessarily', respectively.[1231]

[1224] Privacy Act Review Report 2022 Proposal 281.
[1225] Ibid 287.
[1226] Privacy Act Review Report 2022 287.
[1227] Government Response 19.
[1228] Issues Paper Part 4, Question 4.7. Question 4.8 is addressed in Part 2 of this Report.
[1229] Ibid Part 4, Question 4.9.
[1230] Submission 3 (Anonymous).
[1231] Submission 8 (Meg Webb MLC).

11.5.3 Professor Margaret Otlowski, Emeritus Distinguished Professor Dianne Nicol, and Dr Lisa Eckstein at the Centre for Law and Genetics expressed support for the Privacy Act Review's proposal for the introduction of a statutory tort for serious invasions of privacy in the form recommended by the ALRC Report 123. The authors also noted that the Report 'recommended that this be done in consultation with the states and territories in the interests of ensuring a nationally consistent approach'.[1232]

11.5.4 TasCOSS also supported the introduction of a statutory civil cause of action for interference with privacy and noted that this has been recommended by other reform bodies.

11.5.5 The South Australian Law Reform Institute ('SALRI') submitted its *Report 4: A Statutory Tort for Invasions of Privacy* (2016), which, as touched on above, proposed the enactment in South Australia of a limited cause of action for serious invasions of personal privacy similar to the one proposed by the ALRC—which it recommended extend to the protection of bodily, territorial, information, and communication privacy.[1233] SALRI acknowledged that there would be advantages in developing a consistent national privacy regime but recommended that South Australia lead the way, on the basis that it appeared 'unlikely (at least in the near future) that the Commonwealth will be legislating to establish a national regime' and that a South Australian statute 'could provide leadership' to other State and Territory jurisdictions.[1234]

11.6 The TLRI's view

11.6.1 The TLRI considers that the introduction of a statutory tort for serious invasions of privacy would address a significant gap in privacy protection in Tasmania which appears unlikely to be addressed in common law in the immediate term. As noted above, this view is consistent with recommendations of multiple national and State-based reviews in recent years.

11.6.2 The TLRI shares the view of the ALRC and the Commonwealth Privacy Act Review that it would be most appropriate for a statutory tort to be enacted in a standalone Commonwealth Act, with cross-vesting of Federal jurisdiction, so that it would apply to individuals and agencies across the Commonwealth, States, and Territories, and enable actions to be commenced in both Federal and State and Territory courts.[1235] The TLRI notes the ALRC's view that such an approach would not infringe on the implied limitation on the Commonwealth's power to legislate to impose 'a special disability or burden on the exercise of powers and fulfilment of functions of the states which curtails their capacity to function as governments' ('the *Melbourne Corporation* principle').[1236]

11.6.3 The TLRI considers that, if the Commonwealth does not adopt the proposal of the ALRC and the Privacy Act Review in the near future, further consideration should be given to the introduction of Tasmanian legislation to create a statutory civil cause of action, or statutory tort, of privacy.

[1232] Submission 17 (Centre for Law and Genetics).
[1233] Submission 13 (SALRI) and South Australian Law Reform Institute, *A Statutory Tort for Invasion of Privacy* (Final Report 4, March 2016).
[1234] Ibid 66.
[1235] ALRC, *Serious Invasions of Privacy in the Digital Era* 165–166.
[1236] ALRC, *Serious Invasions of Privacy in the Digital Era* 165–166 and quoting *Fortescue Metals Group Ltd v Commonwealth* (2012) 247 CLR 486, [130] (Hayne, Bell, and Keane JJ).

11.7 Recommendation

Recommendation 63: If a national statutory tort is not adopted by the Commonwealth in the near future, consideration should be given to the introduction of Tasmanian legislation to create a statutory tort of privacy

Appendix 1

State and Territory Protection of Privacy

New South Wales ('NSW')

The *Privacy Committee Act 1975* (NSW) established a body to investigate complaints about the handing of private information by NSW Government bodies. After the passing of the *Privacy and Personal Information Protection Act 1998* (NSW), the Committee was replaced by a Privacy Commissioner. The Act also establishes Information Privacy Principles applicable to NSW public sector agencies (other than health information). These principles are similar, though not identical, to the Australian Privacy Principles ('APPs') in the *Privacy Act 1998* (Cth) ('Privacy Act'). The *Government Information (Information Commissioner) Act 2009* (NSW) establishes an Information Commissioner, separate to the Privacy Commissioner, both of which operate within the Information and Privacy Commission of NSW.

The *Health Records and Information Privacy Protection Act 2002* (NSW) extended protection of personal health information to some private health organisations. The *Workplace Surveillance Act 2005* (NSW) and *Surveillance Devices Act 2007* (NSW) regulate the surveillance of employees and use of surveillance devices generally. Other legislation that relates to privacy includes: the *Adoption Act 2000* (NSW), *Assisted Reproductive Technology Act 2007* (NSW), *Crimes (Forensic Procedures) Act 2000* (NSW), and the *Criminal Records Act 1991* (NSW).

Victoria ('Vic')

The *Privacy and Data Protection Act 2014* (Vic) repeals the *Information Privacy Act 2000* (Vic), establishing the Office of the Victorian Information Commissioner (in place of the Victorian Privacy Commissioner) and containing Information Privacy Principles applicable to Victorian public sector bodies and certain other organisations. The principles are similar to the APPs in the Privacy Act.

Health information handled by both public and private sector bodies is regulated under the *Health Records Act 2001* (Vic). Provisions in relation to personal information and health information are also contained in the *Mental Health and Wellbeing Act 2022* (Vic). Workplace surveillance is regulated by the *Surveillance Devices Act 1999* (Vic), which includes amendments made by the *Surveillance Devices (Workplace Privacy) Act 2006* (Vic).

Victoria is one of the three Australian jurisdictions with a human rights charter. The *Charter of Human Rights and Responsibilities Act 2006* (Vic) includes protection of the right of a person not to have unlawful or arbitrary interference with his or her privacy, family, home, or correspondence. This protection is achieved by mandating that legislation be interpreted consistently with the protected rights (where such interpretation is possible on the text), and by requiring public authorities to act in a way that is compatible with those rights.

Queensland ('Qld')

The *Invasion of Privacy Act 1971* (Qld) regulates credit reporting agents and the use of listening devices in private conversations. The *Information Privacy Act 2009* (Qld) introduced privacy obligations applicable to Queensland Government departments, agencies, and contractors, as well as a separate set of principles applicable to health services. Complaints under the Act are made to the Queensland Office of the Information Commissioner.

Queensland also has a human rights charter. The *Human Rights Act 2019* (Qld) includes protection of the right not to have the person's privacy, family, home, or correspondence unlawfully or arbitrarily interfered with, and not to have the person's reputation unlawfully attacked. As in Victoria, protection

is achieved by setting how legislation is to be interpreted, by requiring public authorities to act in a way that is compatible with the listed rights.

Western Australia ('WA')

Western Australia does not have overarching privacy legislation. The *Health Services Act 2016* (WA) includes a privacy provision that prohibits a person from collecting, using, or disclosing any personal information obtained in the course of their employment. It provides exceptions in certain circumstances, such as where it is done in the performance of their duties or with consent. The *Freedom of Information Act 1992* (WA) also includes some privacy principles related to the disclosure and amendment of personal information held by state and local government agencies. Separately, the *Surveillance Devices Act 1998* (WA) regulates the use of surveillance devices.

South Australia ('SA')

South Australia also does not have legislation providing for general information privacy protection. Instead, it has the Privacy Committee of South Australia, which is established under government proclamation,[1237] as well as the Information Privacy Principles Instruction, which is issued by Premier and Cabinet.[1238] The Committee oversees implementation of the principles by South Australian public sector agencies.

The *Health and Community Services Complaints Act 2004* (SA) establishes the South Australian Health and Community Services Complaints Commissioner. This office resolves complaints about health and community services in South Australia. Complaints are addressed by reference to the *Charter of Health and Community Services Rights*, which includes the right of an individual to have their privacy respected and their personal information kept confidential and secure.[1239]

Separately, the *Surveillance Devices Act 2016* (SA) regulates the use of surveillance devices.

Northern Territory ('NT')

The *Information Act 2002* (NT) is overseen by the Office of the Information Commissioner. The Act includes Information Privacy Principles applicable to public sector agencies. Complaints relating to the privacy of health information can be made to the Health and Community Services Complaints Commission under the *Health and Community Services Complaints Act 1998* (NT). Surveillance devices are regulated by the *Surveillance Devices Act 2007* (NT).

Australian Capital Territory ('ACT')

The *Information Privacy Act 2014* (ACT) establishes a set of Territory Privacy Principles ('TPPs') that govern how ACT public sector agencies handle personal information. Complaints relating to information handling practices and data breach notifications are investigated by the Office of the Australian Information Commissioner ('OAIC') under an arrangement with the ACT Government.

Health records held by ACT Government agencies (including public hospitals) are covered by the *Health Records (Privacy and Access) Act 1997* (ACT). Health record privacy complaints are made to the ACT Human Rights Commission.

[1237] Government of South Australia, Attorney-General's Department, 'State Records; Privacy Committee of South Australia', available at https://archives.sa.gov.au/general-information/privacy-committee/privacy-committee-sa.
[1238] Premier and Cabinet Circular, PC 012 – Information Privacy Principles (IPPs) Instruction, effective from May 2020, available at https://www.dpc.sa.gov.au/resources-and-publications/premier-and-cabinet-circulars/DPC-Circular-Information-Privacy-Principles-IPPS-Instruction.pdf.
[1239] See Health and Community Services Complaints Commissioner, 'HCSCC Charter of Rights', available at https://www.hcscc.sa.gov.au/hcscc-charter-of-rights/.

The ACT is the third Australian jurisdiction with a human rights charter. The *Human Rights Act 2004* (ACT) includes protection of the right not to have the person's privacy, family, home, or correspondence unlawfully or arbitrarily interfered with, and not to have the person's reputation unlawfully attacked. As with Victoria and Queensland, the charter achieves this protection through approaches to interpretation of legislation and by requiring public authorities to act in a way that is compatible with the rights.

Surveillance devices are regulated under the *Listening Devices Act 1992* (ACT).

Appendix 2

Law Reform Projects

The table below records the main law reform projects relating to privacy law in Australia.[1240]

Year	Jurisdiction	Title	Summarised recommendation
1979	Cth	Australian Law Reform Commission, *Unfair Publication: Defamation and Privacy* (Report No 11, June 1979)	Focused on defamation law and the protection of reputation, honour, and dignity. Recommendations focused on making substantial changes to defamation law with a view to improving reputational protection. However, tortious protection for information privacy was also explored, including appropriate remedies. The Commission recognised the normative importance of individual privacy. It found that the law imperfectly protects privacy. It recommended a comprehensive cause of action for misuse of private facts.
1983	Cth	Australian Law Reform Commission, *Privacy* (Report No 22, December 1983)	Privacy was in danger at the time and, even more so, prospectively, with the chief sources of danger being growing official powers, new business practices, and new information technology. It recommended increased regulation to protect private information, providing a draft bill. The *Privacy Act 1988 (Cth)* was passed into law five years later.
2003	Cth	Australian Law Reform Commission, *Essentially Yours: The Protection of Human Genetic Information in Australia* (Report No 96, May 2003)	Made 144 recommendations about how Australia should deal with the ethical, legal, and social implications of new genetics, including how best to protect privacy in this context.
2005	Vic	Victorian Law Reform Commission, *Final Report: Workplace Privacy* (Report, October 2005)	Significant legislative gaps in the protection of privacy in workplaces required regulation at the State level. Recommended enactment of workplace privacy legislation and the establishment of a workplace privacy regulator. This was followed by targeted legislation: *Surveillance Devices (Workplace Privacy) Act 2006* (Vic).
2008	Cth	Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice* (Report No 108, August 2008)	Privacy recognised as a human right which should be protected in spite of other factors such a cost or inconvenience, but should be balanced against important countervailing interests such as freedom of expression and national security. Recommended a federal statutory cause of action for a serious invasion of privacy (aside from the *Privacy Act 1988* (Cth)).

[1240] See summaries and critical commentary at T Wilson 'Privacy Law Recommended' (2007) 4 *Privacy Law Bulletin* 38; Normann Witzleb, 'A Statutory Cause of Action for Privacy? A Critical Appraisal of Three Recent Australian Law Reform Proposals' (2011) 19 *Torts Law Journal* 104; Normann Witzleb 'Another Push for an Australian Privacy Tort' (2020) 94(10) *Australian Law Journal* 765.

Year	Jurisdiction	Title	Summarised recommendation
2008	Qld	FOI Independent Review Panel, *Solomon Report: The Right to Information, Reviewing Queensland's Freedom of Information Act* (Report, June 2008)	While this was a review of freedom of information laws (also known as right to information laws in Tasmania), some recommendations were made to strengthen information privacy protections.
2009	NSW	NSW Law Reform Commission, *Invasion of Privacy* (Report No 120, April 2009)	As part of a uniform law initiative in Australia, recommended that NSW should amend the *Civil Liability Act 2002* (NSW) to provide a cause of action for invasion of privacy in the terms of the draft legislation appended by the Commission to this report. Ultimately, however, the Civil Liability Amendment (Privacy) Bill 2009 (NSW) was not passed into law.
2010	NSW	NSW Law Reform Commission, *Protecting Privacy in New South Wales* (Report No 127, May 2010)	Focused on privacy and personal information regulation, rather than a comprehensive civil remedy for interference with privacy.
2010	Vic	Victorian Law Reform Commission, *Surveillance in Public Places* (Report No 18, August 2010)	Recommended that the Parliament should enact new laws that promote the responsible use of surveillance devices in public places, including creating statutory causes of action covering serious invasion of privacy by misuse of private information, and serious invasion of privacy by intrusion upon seclusion.
2014	Cth	Australian Law Reform Commission, *Serious Invasions of Privacy in the Digital Era* (Report No 123, June 2014)	Recommended the introduction of a single statutory tort of interference with privacy, covering both information and physical privacy.
2016	SA	South Australian Law Reform Institute, *Final Report: A Statutory Tort for Invasion of Privacy* (Final Report 4, March 2016)	Found that protections available in South Australia for interferences with a person's privacy were inadequate. It found that, although previous attempts at reform of this kind in South Australia were unsuccessful, the impetus for reform is now different as the people of South Australia are more vulnerable to invasions of privacy than ever before, particularly due to technological advances.

Year	Jurisdiction	Title	Summarised recommendation
2016	NSW	Legislative Council Standing Committee on Law and Justice, Parliament of NSW, *Remedies for the Serious Invasion of Privacy in New South Wales* (Report, March 2016)	Found that current privacy provisions were inadequate, and recommended the introduction of statutory causes of action for serious invasions of privacy.
2017	Qld	Department of Justice and Attorney-General, *Report on the Review of the Right to Information Act 2009 and Information Privacy Act 2009* (Report, October 2017)	Made a range of recommendations for amendment of *Information Privacy Act 2009* (Qld), including extending the Act to include subcontractors and to clarify privacy processes.
2019	Cth	Australian Competition and Consumer Commission, *Digital Platforms Inquiry* (Final Report, June 2019)	Found that data protection and related privacy interests require stronger legal protection to address growing incursions through the use of digital platforms, particularly through the commodification of personal data.
2019	NSW	NSW Department of Communities and Justice, *Mandatory Notification of Data Breaches by NSW Public Sector Agencies* (Discussion Paper, July 2019)	Discussed the introduction of a mandatory reporting scheme for data breaches by NSW public sector bodies.
2020	Qld	Queensland Law Reform Commission, *Review of Queensland's Laws Relating to Civil Surveillance and the Protection of Privacy in the Context of Current and Emerging*	Recommended the replacement of existing regulation on the use of surveillance devices by all persons.

Year	Jurisdiction	Title	Summarised recommendation
		Technologies (Report No 77, February 2020)	
2021	Cth	Australian Human Rights Commission, *Human Rights and Technology* (Final Report, June 2021)	Focused on protection from the use of artificial intelligence and its implications, including the question of how best to protect privacy in view of these growing concerns.
2022	Vic	Victorian Law Reform Commission, *Stalking, Harassment and Similar Conduct* (Final Report, September 2022)	Focused on behaviours that constitute, or are similar to, stalking and harassment, and questioned whether existing legal protections are adequate to address such conduct.
2022	NSW	Legislative Council Select Committee on the Impact of Technological and Other Change on the Future of Work and Workers in New South Wales, Parliament of New South Wales, *Final Report: Workplace Surveillance and Automation* (Report No 2, November 2022)	Recommendations for improving workplace surveillance given recent and rapid technological advancements and automation. Recommends updating *Workplace Surveillance Act 2005* (NSW) to improve privacy protections for workers, consultation and consent requirements, and dispute resolution processes.
2022	WA	Department of Premier and Cabinet (WA), *Privacy and Responsible Information Sharing Fact Sheet* (Document, 14 December 2022)	WA Government drafting new legislation to reform privacy protections, including introducing Information Privacy Principles, Privacy Commissioner, mandatory data breach notification scheme, and mechanisms for responsible information sharing within government.

Year	Jurisdiction	Title	Summarised recommendation
2022	Qld	Department of Justice and Attorney- General (Qld), *Consultation Paper: Proposed Changes to Queensland's Information Privacy and Right to Information Framework* (Report, June 2022) Consultation closed 22 July 2022	Current Bill proposing substantive changes *to Information Privacy Act 2009* (Qld). (*Information Privacy and Other Legislation Amendment Act 2023*, passed December 2023 but not yet assented to).
2023	Cth	Attorney-General's Department (Cth), *Privacy Act Review Report* (16 February 2023) Attorney-General's Department (Cth), *Government Response to the Privacy Act Review Report* (28 September 2023)	Detailed reform proposals to strengthen the protection of personal information and the control individuals have over their information.
2023	Vic	Integrity and Oversight Committee (Victorian Parliament), Inquiry into the *Operation of the Freedom of Information Act 1982* (October 2023)	Operation and effectiveness of the *Freedom of Information Act 1982* (Vic) including efficient and timely mechanisms for people to access their own personal and health information.
2023	Qld	Department of Justice and Attorney- General (Qld Government), *Civil Surveillance Reforms* (Consultation Paper, April 2023) Consultation closed 31 May 2023	Considering recommendations of Queensland Law Reform Commission's *Review of Queensland's Laws Relating to Civil Surveillance and the Protection of Privacy in the Context of Current and Emerging Technologies* (Report No. 77, February 2020). Consulting on possible repeal of *Invasion of Privacy Act 1971* (Qld) and enactment of QLRC's draft Surveillance Devices Bill. Seeking feedback on staged approach to implementing civil surveillance reforms, use and communication/publication prohibitions, and the need for specific workplace surveillance legislation (as in NSW, Vic, ACT).