TASMANIA
LAW REFORM
INSTITUTE

Review of Privacy Laws in Tasmania

ISSUES PAPER NO 32

MARCH 2023

www.utas.edu.au/law-reform/publications/ongoing-law-reform-projects

Cite as: Tasmania Law Reform Institute, *Review of Privacy Laws in Tasmania* (Issues Paper No 32, March 2023)

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: Professor Gino Dal Pont (Acting Chair, 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), Craig Mackie (appointed by the Tasmanian Bar Association), 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) 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.

How to respond

The Tasmania Law Reform Institute invites responses to the various issues discussed in this Issues Paper. There are a number of questions posed by this Issues Paper to guide your response. **Respondents can choose to answer any or all of those questions in their submissions.** Respondents can also suggest alternative options for reform or raise other relevant matters in their responses.

There are a number of ways to respond:

- By filling in the Submission Template

  The Template can be filled in electronically and sent by email or printed out and filled in manually and posted. The Submission Template can be accessed at the Institute's webpage

  <https://www.utas.edu.au/law-reform/publications/ongoing-law-reform-projects>.

- By providing a more detailed response to the Issues Paper

  The Issues Paper poses a series of questions to guide your response—you may choose to answer, all, some, or none of them. Please explain the reasons for your views as fully as possible.

- By requesting a meeting

  If you do not wish to respond in writing you can phone or write and ask to speak with a researcher instead. You can then make your submission by phone, through an online meeting platform, or in person, either individually or as part of a group.

The Institute uses all submissions received to inform its research. Submissions may be referred to or quoted from in a TLRI final report which will be printed and also published on the Institute's website. Extracts may also be used in published scholarly articles and/or public media releases. However, if you do not wish your response to be referred to or identified, the Institute will respect that wish.

Therefore, when making a submission to the Institute, please identify how you would like it to be treated based on the following categories:

1. Public submission—the Institute may refer to or quote directly from the submission, and name you as the source of the submission in relevant publications.

2. Anonymous submission—the Institute may refer to or quote directly from the submission in relevant publications, but will not identify you as the source of the submission.

3. Confidential submission—the Institute will not refer to or quote directly from the submission, but may aggregate information in your submission with other submissions for inclusion in any report or publication. Confidential submissions will only be used to inform the Institute generally in their deliberations of the particular issue under investigation, and/or provide publishable aggregated statistical data.

After considering all responses and stakeholder feedback it is intended that a final report, containing recommendations, will be published.

Providing a submission is completely voluntary. You are free to withdraw your participation at any time, by contacting Kira White on (03) 6226 2069 or email Law.Reform@utas.edu.au. You can withdraw without providing an explanation. However, once the report has been sent for publication, it will not be possible to remove your comments.

All responses will be held by the Tasmania Law Reform Institute for a period of five (5) years from the date of the first publication and then destroyed. Electronic submissions will be stored on a secure, regularly backed-up University network drive. Hard copy submissions will be stored in a locked filing cabinet. At the expiry of five years, submissions be deleted from the server, in the case of electronic submissions, or shredded and securely disposed of in the case of paper submissions.

Electronic submissions should be emailed to: Law.Reform@utas.edu.au

Submissions in paper form should be posted to:

Tasmania Law Reform Institute

Private Bag 89

Hobart, TAS 7001

Inquiries about the study should be directed to Professor Jeremy Prichard at the above address, or by telephoning (03) 6226 2069, or by email to Law.Reform@utas.edu.au.

CLOSING DATE FOR RESPONSES: 11 July 2023

This study 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].

Acknowledgments

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

This Issues Paper 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 paper was edited and prepared for publication by Dr Nina Hudson. Ongoing administrative and management of the Inquiry has been provided by Kira White.

Background and Terms of Reference

This Inquiry 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.

The issue of privacy protection is topical in view of the matters raised in the Terms of Reference below and other developments, such as national data breaches relating to organisations such as Medicare and Optus.

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.

The Terms of Reference are for the TLRI to inquire into, review and report on:

1. 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;
2. 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
3. models that enhance and protect privacy in other jurisdictions (in Australia and overseas).

In undertaking this reference, the TLRI will 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.

The TLRI will 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.

Nature and scope of the Issues Paper

Scope and structure

The content for this Issues Paper was finalised in January 2023. This preceded the 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'). Accordingly, this Issues Paper does not consider the findings of the report as to options for reforming the Privacy Act (particularly relevant to the contents of Part 2, noted below). However, the findings of the Commonwealth report will be considered in the drafting of the TLRI Final Report and the formulation of recommendations.

- Part 1 (pages 1 to 6) introduces readers to the concept of privacy protection and gives an overview of existing legal frameworks for privacy protection in Tasmania, Australia, and internationally.
- Part 2 (pages 7 to 45) discusses the scope, operation, and enforcement of privacy protection under the frameworks introduced in Part 1, focusing on information held by government agencies. It compares the protections in Tasmania under the *Personal Information Protection Act 2004* (Tas) ('PIPA') with those in other Australian jurisdictions, particularly under the Privacy Act. Part 2 also considers possible future reforms of these frameworks and examines international developments, including the European Union's *General Data Protection Regulation 2016/679* ('GDPR').
- Part 3 (pages 47 to 51) explores different provisions in legislation other than the PIPA that affect how government-held information can be used and shared. It analyses how these provisions affect information privacy and draws comparisons with similar laws in other jurisdictions.
- Part 4 (pages 52 to 66) broadens the scope beyond government-held information to consider various types of privacy protections under legislation, as well as case law. It discusses 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. Part 4 concludes by considering the introduction of a comprehensive civil remedy for interference with privacy and sets out questions about the appropriate model for law reform.

Summary

This Issues Paper provides background, context, and considerations regarding privacy laws in Tasmania. The aim is to facilitate informed discussion about how privacy can best be legally protected, given the rapid advances in information technology, changing community perceptions about the importance of privacy, and growing legislative regulation of various matters.

The Paper adopts a broad working definition of privacy ([1.1.2]) 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 ([1.2]). Different legislation may interact to affect privacy protections (Part 3). The applicability of regulations at the Australian federal level under the Privacy Act and the international level, for example under the European Union's *General Data Protection Regulation 2016/679* ('GDPR'), create further complexity in the landscape of privacy protection.

The primary privacy framework in Tasmania is the *Personal Information Protection Act 2004* (Tas) ('PIPA') which binds government agencies and their contractors. It protects the information privacy of government-held information, primarily through prescribing ten 'Personal Information Protection Principles' 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.

Regarding scope, for example, the PIPA does not cover non-government organisations such as for-profit businesses ([2.2.3]); it does not contemplate the possibility of de-identified information being re-identified with the help of additional information ([2.2.22]–[2.2.28]); it does not protect unsolicited personal information—information that comes into the hands of government agencies or their contractors without a deliberate effort on their part to collect it ([2.3.51]); and it does not grant special protections for biometric information, unlike the Commonwealth law ([2.2.43]).

Advances in technology can exacerbate the impact of these gaps. For example, the lack of special protection for biometric information may pose a greater risk to individuals as technologies increase in sophistication, such as facial recognition.

This Paper suggests potential reforms to the PIPA aimed at improving privacy protection, such as by allowing individuals to have a right to object to their information being processed, and a right to request their information be erased ([2.3.60]–[2.3.90]).

However, some of the most important gaps relate to the enforcement of the PIPA, rather than its scope. In particular, there is limited ability for an aggrieved individual to seek review of decisions about whether or not there has been a breach ([2.4.7], [2.4.14]); there are no penalties imposed for breaching obligations ([2.4.10]); there is no mandatory data breach notification scheme that compels information handlers to notify an individual where a breach of their privacy has occurred ([2.4.21]); there is no ability for those handling complaints to order compensation ([2.4.8]); and there is no private right of action that allows an individual to go to court to seek damages for financial or non-financial harm suffered as a result of the breach.

These gaps, together with the fragmented landscape of protections under both legislation and general law, means that some circumstances that endanger privacy may fall between the cracks of legal regulation ([4.4.3]). This raises questions as to whether there may be a case for creating a civil statutory cause of action (and remedy) for interference with privacy ([4.4]). If such a remedy were to be created, consideration is given to whether it should be comprehensive (applying independently of the context in which the interference occurs), apply in place of or in addition to the existing suite of remedies, and allow individuals to seek redress in court when they have suffered harm.

In discussing the strengths and weaknesses of the PIPA and privacy laws more generally, this Paper seeks 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.

List of acronyms and abbreviations

In this Issues Paper, language that is consistent with relevant Acts is used wherever possible. The following is a complete list of acronyms, abbreviations, and key terms used:

ACCC	Australian Competition & Consumer Commission
ACT	Australian Capital Territory
ADEPT	Administrative Data Exchange Protocol for Tasmania
AHRC	Australian Human Rights Commission
ALRC	Australian Law Reform Commission
APPs	Australian Privacy Principles
ICCPR	*International Covenant on Civil and Political Rights*
GDPR	European Union's *General Data Protection Regulation 2016/679*
NSW	New South Wales
OAIC	Office of the Australian Information Commissioner
PIPA	*Personal Information Protection Act 2004* (Tas)
Privacy Act	*Privacy Act 1988* (Cth)
PIPPs	Personal Information Protection Principles
RPA	Remotely Piloted Aircraft
TLRI	Tasmania Law Reform Institute
UAV	Unmanned Aerial Vehicles

List of questions

The TLRI welcomes your response to any individual question or to all questions contained within this paper. A full list of the consultation questions is contained below with page references for questions that relate to different parts of the Issues Paper.

Chapter 2—Privacy protection: Scope and application of the PIPA (pp. 7–22)	
2.1	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'?
2.2	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?
2.3	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?
2.4	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?
2.5	Are the other categories of information, including health and other forms of sensitive information suitable?
2.6	Are the exceptions, including the process for declaring and publishing public benefit exemptions, suitable?
Chapter 2—Privacy protection: Personal Information Protection Principles (pp. 23–38)	
2.7	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?
2.8	Are there any other amendments to the PIPPs that you think should be made?
2.9	Should any of the other potential reforms be introduced, including: a. fairness and reasonableness requirements; b. a right to object; c. a right to be forgotten; d. specific restrictions on the use of artificial intelligence in automated administrative decision-making; or e. strengthened notice and consent requirements?

Chapter 2—Privacy protection: Complaints, monitoring and enforcement (pp. 39–45)	
2.10	How effective is the current complaints process in enforcing obligations under the PIPA?
2.11	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?
2.12	What other remedies should be available to individuals affected by a breach of the PIPA?
2.13	Are there other forms of enforcement action that should be introduced?
2.14	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?
2.15	Should a form of data breach notification requirement be introduced? If so, what models of mandatory reporting schemes should be considered?
Chapter 3—Other legislation impacting the privacy of government-held information (pp. 47–51)	
3.1	Should legislation providing for the application of minimum privacy safeguards be introduced to apply to all information sharing within and between government bodies?
3.2	If such legislation should be introduced, how should the safeguards be enforced?
Chapter 4—Other protections of privacy (pp. 52–66)	
4.1	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?
4.2	Should there be stronger legislative protection, including through the introduction of new statutes in Tasmania, against governmental (particularly police) surveillance in general?
4.3	Should there be stronger legislative protection, including through the introduction of new statutes in Tasmania, against workplace surveillance in particular?
4.4	Should there be specific protection against interference with physical privacy through the use of drones (RPAs and UAVs)?
4.5	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?
4.6	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?

4.7	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?
4.8	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?
4.9	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?

Part 1

1 Privacy protection

This Part provides an overview of privacy protection. It first outlines the meaning of 'privacy' and the source of a right to privacy. It then defines the scope and benefits of privacy protection. Finally, it summarises the legal frameworks applicable in Tasmania, Australia, and internationally. Part 2 analyses in detail the key framework, the *Personal Information Protection Act 2004* (Tas) ('PIPA').

1.1 What is 'privacy'?

1.1.1 The overarching question referred to the TLRI is whether the current privacy laws in Tasmania are adequately protective. The meaning of privacy is central to this question. Defining the scope of privacy has proved an 'elusive task',[1] and it is generally described through several different typologies or categories.

1.1.2 In its 2008 report into privacy laws, the Australian Law Reform Commission ('ALRC') adopted four overlapping categories of privacy protection, which are also adopted as working definitions in this Issues Paper. They are as follows:

- *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.[2]

1.1.3 As a note on terminology, rights to bodily and territorial privacy may be otherwise known as 'rights to seclusion'. Intrusions on seclusion include watching, listening to, or recording what a person does in private.[3]

1.2 Scope and benefits of privacy protection

1.2.1 Determining the extent to which society protects privacy is important. The protection of privacy interrelates with:

[1] Australian Law Reform Commission ('ALRC'), *Privacy*, ALRC 22 (1983).
[2] 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 (Web Page) <https://www.privacyinternational.org/survey/phr2000/overview.html>.
[3] ALRC, *Serious Invasions of Privacy in the Digital Era* (Report No 123, June 2014) [5.18].

- Safeguarding human dignity[4] and individual autonomy[5]—the ability to control and choose how information about yourself is provided to others may be a precondition for individual liberty.[6]
- Psychological well-being and security, fostering intimacy, and promoting intellectual development.[7]
- Social benefits—enabling social interaction, encouraging participation in democratic processes, encouraging cultural and critical innovation, and assisting cohesion in pluralistic communities.[8]

1.2.2 The *International Covenant on Civil and Political Rights*[9] ('ICCPR') provides for a right to privacy. Australia has signed and ratified the ICCPR, which means that it has consented to be bound to it; however, in order for a right under international law to be enforceable domestically it must be introduced under Australian law (see [1.4.1] below). Article 17 prohibits governments from interfering with a person's privacy and obliges governments to take positive steps to protect against interference by others.[10] 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.[11]

1.2.3 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, which details the circumstances when such government action is permitted and facilitates some form of review or accountability.[12] 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.[13]

---

[4] Charles Fried, 'Privacy' (1968) 77(3) *Yale Law Journal* 475.
[5] Kirsty Hughes, 'A Behavioural Understanding of Privacy and Its Implications for Privacy Law' (2012) 75(5) *Modern Law Review* 806.
[6] Alan F Westin, *Privacy and Freedom* (Atheneum Press, 1967).
[7] 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*').
[8] Ibid 687.
[9] *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').
[10] 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*').
[11] ICCPR (n 9) 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.
[12] *General Comment No 16* (n 10) [8].
[13] 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).

1.3 Privacy protection in Tasmania

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

1.3.2 Information privacy, at least as far as information held by Tasmanian government agencies, is primarily protected through the PIPA. Other laws also impact the government's ability to access, use or disclose personal information. These may be general in scope, such as the *Right to Information Act 2009* (Tas), or applicable only in specific contexts.

1.3.3 Beyond government-held information, there are also information privacy rights relating to a person's health information, as found in the *Health Complaints Act 1995* (Tas) and the subsequently developed *Tasmanian Charter of Health Rights and Responsibilities*. The Act and the Charter relate to consumers of health services, and apply to both public and private health service providers.

1.3.4 Bodily and territorial privacy, otherwise known as rights to seclusion, are protected through various sources of law. These are considered in detail in Part 4, and include:

- 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.
- Other 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) and the *Disability Services Act 2011* (Tas), which correspondingly mandate that children and persons with disability must be treated in a manner respecting their dignity and privacy.
- The general law, where Tasmanian courts have made references to privacy in several important contexts.

1.3.5 This Paper considers these protections and raises questions about whether and how they may be reformed to better protect the privacy of Tasmanians.

1.4 Privacy protection in other Australian jurisdictions

1.4.1 The *Privacy Act 1988* (Cth) ('Privacy Act') is the main privacy legislation operating at the federal level in Australia. The introduction of this Act partially implemented Australia's obligations under article 17 of the ICCPR.[14] It should be noted that, in Australia, such implementing legislation is necessary before international treaties have any domestic legal effect—international obligations are not automatically enforceable in domestic law.

1.4.2 Developed in response to the ALRC's Privacy Report,[15] the Privacy Act introduced various privacy principles applicable to the handling of personal information by Commonwealth government agencies. It also established a Privacy Commissioner to investigate complaints against mishandling.

[14] *Privacy Act 1988* (Cth). In addition to partially implementing the ICCPR, the *Privacy Act 1988* (Cth) also implemented obligations under the Organisation 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].
[15] ALRC, *Privacy* (n 1).

1.4.3 In 2000, the Privacy Act was amended to establish a separate set of principles applicable to some private sector organisations.[16] In 2012 after another ALRC inquiry,[17] the Act was further amended to provide a common set of privacy principles applicable to both the Commonwealth public sector and private organisations. These are known as the Australian Privacy Principles ('APPs').[18]

1.4.4 At the state and territory level, all jurisdictions except Western Australia and South Australia have general legislation regulating how the public sector can handle personal information. In the states and territories where such general legislation exists, these laws broadly provide some variation on the Commonwealth APPs set out in the Privacy Act. Further, similar to the federal law, complaints are investigated by an independent body. Appendix 1 provides a description of each state and territory's framework. Notably, 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.

1.4.5 While there are some similarities between separate state and territory frameworks, consistency across privacy protections is a concern. Indeed, the ALRC has discussed the importance of consistent privacy regulation:

> 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.[19]

1.4.6 To achieve consistency, the ALRC recommended that the Commonwealth legislate 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.[20] State and territory governments were encouraged to promote and maintain uniformity by agreeing to implement legislation for a set of common privacy principles applicable to government agencies.[21]

1.4.7 Consistency has been similarly considered as an important goal for law reform in reviews of privacy legislation in various Australian 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.[22]
- 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.[23]

[16] *Privacy Amendment (Private Sector) Act 2000* (Cth), which commenced on 21 December 2001.
[17] ALRC, *For Your Information* (n 2).
[18] *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth), which commenced on 12 March 2014.
[19] ALRC, *For Your Information* (n 2) [3.13].
[20] Ibid 218–12, recommendations 3-1, 3-2, 3-3.
[21] Ibid 219–20, 224, recommendations 3-4, 3-5.
[22] 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).
[23] Government of Western Australia, *Privacy and Responsible Information Sharing for the Western Australian Public Sector* (Discussion Paper, 2019).

- More recently, 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.[24]
- The review of the Commonwealth Privacy Act has also emphasised the value of consistency.[25] In its submission to the review, the Office of the Australian Information Commissioner ('OAIC') recommended that harmonisation should be a key goal when designing any laws that purport to address privacy issues. The OAIC suggested that privacy protections in any such federal, state, or territory laws be commensurate with those under the Privacy Act.[26]

1.4.8 Given the emphasis on consistency in privacy regulation, this Issues Paper takes a comparative approach to potential reform of Tasmania's laws. Comparisons will be drawn between Tasmanian legislation and legislation in other Australian jurisdictions, with a focus on the Commonwealth APPs. Where relevant, lessons will also be taken from international frameworks.

1.5 Reviews of Australian privacy regulation

1.5.1 A number of law reform projects in Australian jurisdictions have explored the value of privacy laws, and the extent to which they protect privacy. These reviews are set out in Appendix 2.

1.5.2 In October 2020, the Commonwealth Attorney-General's Department commenced a review of the Privacy Act.[27] The review covers 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 whether there should be a separate Commonwealth statutory civil remedy for interference with privacy.

1.5.3 Where relevant, this Issues Paper pays regard to matters raised in the Commonwealth review, and in some prominent submissions to that inquiry—in particular, the OAIC's submission. The outcomes of the Commonwealth review are contained in a report that was released on 16 February 2023.[28] As this Issues Paper was finalised in January 2023, it does not consider the findings of the report as to options for reforming the Privacy Act. However, the findings of the Commonwealth report will be considered in the drafting of the TLRI Final Report and the formulation of recommendations.

1.6 International comparisons

1.6.1 The interaction between individuals, organisations, and businesses around the world means that certain privacy regulations in international jurisdictions may also be relevant to privacy protection in Tasmania.

[24] Crime and Corruption Commission (Queensland), *Operation Impala: Report on Misuse of Confidential Information in the Queensland Public Sector* (Report, February 2020) recommendation 16.
[25] Attorney-General's Department, *Privacy Act Review* (Issues Paper, October 2020) 83.
[26] See Office of the Australian Information Commissioner ('OAIC'), *Privacy Act Review: Submission by the Office of the Australian Information Commissioner* (Issues Paper, 11 December 2020) ('*Submission to Privacy Act Review*'). The OAIC also recommended that national consistency of privacy regulation should be a key goal of the Council of Attorneys-General by establishing a working group to consider amendments to state and territory privacy laws to achieve alignment with the Privacy Act (recommendation 3).
[27] 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>.
[28] Attorney-General's Department, *Privacy Act Review: Report 2022* (Report, February 2023).

1.6.2 The *General Data Protection Regulation 2016/679* ('GDPR')[29] of the European Union binds any public and private organisation that controls or processes personal information and regulates how it can process that personal information. It was intended to harmonise data protection laws across the European Union to build legal certainty for businesses and enhance trust in online services.[30] It implements the right to the protection of personal data under article 8 of the *Charter of Fundamental Rights of the European Union*, which requires such data to be:

> processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.[31]

1.6.3 The GDPR also applies to organisations that offer goods or services to, or monitor the behaviour of, individuals within the European Union.[32] It may therefore apply to activities of the Tasmanian Government and of Tasmanian organisations intending to do business with the European Union.

1.6.4 Another point of interaction is cross-jurisdiction data transfers. Under the GDPR, personal data can only be freely transferred outside of the European Union if the receiving country or organisation provides for an adequate level of privacy protection. If this requirement is not met, as is the case for Australia, data can only be transferred where the European Union party provides appropriate safeguards to ensure that the individual in the information has enforceable rights and remedies.[33] The Privacy Act review has considered whether the Commonwealth law should be amended to offer protections deemed adequate under the GDPR, so as to allow an adequacy arrangement that would authorise the free transfer of personal data between the two jurisdictions.

1.6.5 The GDPR sets a high standard for data protection[34] and has served as a model for legislation in other jurisdictions.[35] In its submission to the Privacy Act review, the OAIC has referred to the GDPR as a relevant comparator both in terms of an Australia-European Union adequacy arrangement and also in considering possible reforms to the Commonwealth privacy principles.[36] The GDPR is therefore relevant to this Issues Paper in two ways. First, Tasmanian entities are potentially subject to its requirements in dealings with the European Union. Second, the GDPR serves as a comparator for identifying potential issues for reform and as an example of how those issues have been approached in other jurisdictions.

---

[29] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with regard to the Processing of Personal Data and on the Free Movement of such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation)* [2016] OJ L 119/1 ('GDPR').

[30] European Commission, 'Joint Statement on the Final Adoption of the New EU Rules for Personal Data Protection' (Press Release, 14 April 2016).

[31] *Charter of Fundamental Rights of the European Union* [2012] OJ C 326/02.

[32] GDPR (n 29) art 3.

[33] Under the GDPR, personal data can only be transferred outside the EU to countries or organisations that provide an adequate level of privacy protection. However, as Australia has not been designated as meeting this requirement, transfers of personal data are conditioned on the enforceability of individual rights within the GDPR and availability of effective remedies: GDPR (n 29) arts 45, 46.

[34] See OAIC, *Submission to Privacy Act Review* (n 26) [8.36].

[35] See, eg, the *California Consumer Privacy Act*: Cal Civ Code § 1798.100 (West 2018).

[36] See, eg, OAIC, *Submission to Privacy Act Review* (n 26) 116.

Part 2

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

2.1 Introduction

2.1.1 The *Personal Information Protection Act 2004* (Tas) ('PIPA') is the primary law for the protection of information privacy in Tasmania, at least as regards information held by Tasmanian government agencies. The PIPA was passed in 2004 with broad bi-partisan support.[37] 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'.[38]

2.1.2 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'[39] in light of the growth of the information economy and increasing use of the internet to deliver government services. It followed an expansion of Commonwealth privacy protection from the public sector to the private sector, and reflected similar legislation in NSW, Victoria and the Northern Territory.

2.1.3 The PIPA generally requires public authorities and their contractors to comply with 10 Personal Information Protection Principles ('PIPPs') when handling personal information, though there are exceptions both within the PIPA and in other legislation. The PIPPs are discussed in detail below at [2.3]. Briefly, they relate to:

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.

2.1.4 Complaints relating to a contravention of the PIPPs can be made to the Ombudsman, who can deal with the matter themselves or refer it to another person, body or authority. If the Ombudsman finds a contravention, this advice and any recommendations are provided to the Minister in charge of administering the PIPA[40] and tabled in both Houses of Parliament. These mechanisms are discussed in detail below at [2.4].

---

[37] See Tasmania, *Parliamentary Debates*, House of Assembly, 20 October 2004, pt 2, 62–4, 96–8.
[38] See the Second Reading speech for the Personal Information Protection Bill 2004 (Tas): Tasmania, *Parliamentary Debates*, House of Assembly, 20 October 2004, 63.
[39] Ibid 62.
[40] Prescribed in the Act as the Minister for Justice and Industrial Relations: *Personal Information Protection Act 2004* (Tas) s 24 ('PIPA').

2.1.5 The following sections dissect various aspects of the PIPA and draw comparisons with privacy laws in other jurisdictions. To highlight potential areas of reform, issues relating to new technologies are identified where relevant.

2.2 Scope and application of the PIPA

Bodies subject to the PIPA

2.2.1 The PIPA broadly applies to state public authorities and some government contractors, referring to these bodies as 'personal information custodians'.[41] For the purposes of the PIPA, the meaning of 'public authority' is adopted from the *Right to Information Act 2009* (Tas) and includes:

- an Agency (including a government department or a state authority);
- 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;
- a Government Business Enterprises; and
- a Council-owned or State-owned company.[42]

2.2.2 Certain public bodies are exempt from the PIPA, either generally or in the course of their official functions. This includes courts and tribunals in the exercise of judicial or quasi-judicial functions or powers, office-holders and registries of such courts and tribunals, the Solicitor-General and their employees, as well as the Director of Public Prosecutions and their employees.[43] Personal information can also be disclosed to various public legal officers and employees for the purpose of obtaining legal advice.[44]

2.2.3 For private or non-government bodies, the PIPA applies only in a limited way. Those bodies must follow the PIPPs only where they have entered into a contract with a public authority and that contract involves the collection, use, or storage of personal information.[45] In such cases, they are deemed personal information custodians and must comply with the PIPPs. Importantly, this applies to all their dealings with personal information—not only those dealings that relate to personal information collected, used, or stored under the contract in question.

2.2.4 One example is where a public authority outsources some aspect of personal information management to a private organisation that provides cloud computing services.[46] Another example is when a public authority contracts 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.

---

[41] Note that public information custodians can also be prescribed in regulations, but at present there are no regulations for the PIPA.
[42] PIPA (n 40) s 3 ('public authority'); see *Right to Information Act 2009* (Tas) s 5.
[43] Ibid s 7.
[44] Ibid s 12A.
[45] See ibid s 3 (definition of 'personal information custodian'). See also ibid s 17 about the obligation to comply with the PIPPs.
[46] Note that use of cloud storage may come within the terms of section 12 of the PIPA, which provides for the efficient storage and use of basic information. See further the discussion of 'basic personal information' below at [2.2.52]–[2.2.54].

2.2.5 Private bodies may also be bound by legislative privacy protections if they are a health service provider. Health information is discussed below at [2.2.34]–[2.2.41]. Some aspects of health information privacy are protected under the PIPA, while others are regulated under the *Tasmanian Charter of Health Rights and Responsibilities* developed under the *Health Complaints Act 1995* (Tas). These frameworks are discussed below at [4.2].

2.2.6 Other states and territories with information privacy legislation[47] generally limit the extent to which protections apply beyond the public sector[48] in similar ways. As in Tasmania, in other jurisdictions the private bodies that typically must comply with the legislative obligations are private health service providers and government contractors.

2.2.7 Private health service providers in NSW, Victoria, and the Australian Capital Territory ('ACT') must comply with both federal and state or territory privacy laws when handling health information.[49]

2.2.8 Meanwhile, in Victoria and Queensland when private contractors are engaged by government agencies as service providers, the extent to which privacy principles apply is more limited compared to Tasmania. In Tasmania, the protections apply automatically when the contractor enters into an outsourcing arrangement with a government agency. However, Victorian or Queensland agencies must take positive steps to bind the contractor to the privacy principles.[50]

- In Victoria, a government contractor is bound only where the contract contains a term providing for this restriction.[51] This contractual term also impacts 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.[52]
- Similarly, in Queensland, a government contractor is bound only where the government agency has taken all reasonable steps to ensure this.[53] If such reasonable steps have not been taken, the government agency remains responsible for breaches of privacy.

[47] All states and territories, other than Western Australia and South Australia.
[48] *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. The Western Australian government is currently consulting on privacy and responsible information sharing legislation for the public sector (see <https://www.wa.gov.au/government/privacy-and-responsible-information-sharing>). South Australia has an administrative scheme under the Information Privacy Principles Instruction (SA).
[49] *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.
[50] *Privacy and Data Protection Act 2014* (Vic) ss 13(1)(j), 17(2); *Information Privacy Act 2009* (Qld) ss 34–7.
[51] *Privacy and Data Protection Act 2014* (Vic) ss 13(1)(j), 17(2).
[52] Ibid s 17(4).
[53] *Information Privacy Act 2009* (Qld) ss 34–7.

Obligations under Commonwealth privacy law for Tasmanian bodies

2.2.9 Separate from the PIPA, information privacy obligations may also be imposed on Tasmanian bodies by the *Privacy Act 1988* (Cth) ('Privacy Act'), which as noted at [1.4.3], establishes a set of Australian Privacy Principles ('APPs'). While the federal law is intended to not affect state or territory laws that regulate personal information in a way that can operate concurrently with the federal law,[54] there are some areas of potential overlap.

2.2.10 The APPs apply to 'APP entities', namely Commonwealth government agencies and various non-government organisations.[55] The latter encompasses 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 $3,000,000.[56]

2.2.11 The definition of 'organisation' exempts some entities from the operation of the Privacy Act. This includes political parties registered under the *Commonwealth Electoral Act 1918* (Cth)[57] and small businesses operators as defined in section 6D of the Privacy Act. It should be noted that the current review of the Privacy Act has questioned whether the small business exemptions which limit that Act's application to the private sector should be removed or amended.[58] The Office of the Australian Information Commissioner ('OAIC') recommended that the exemption be removed subject to an appropriate transition period.[59]

2.2.12 State or territory public authorities are also generally exempt from the operation of the Privacy Act.[60] Similarly, contractors engaged by state public authorities to provide services are exempt, but only in relation to acts that are done in order to fulfil obligations under the state contract.[61] For acts outside of their contractual obligations, 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 $3,000,000 and hence be subject to the Commonwealth APPs, and also be party to a personal information contract with the Tasmanian government and hence generally subject to the Tasmanian PIPPs.

2.2.13 The concurrent operation of the Privacy Act and the PIPA may give rise to complex constitutional questions about consistency between federal and state and territory laws, and it is beyond the scope of this Issues Paper to analyse these questions. However, it is worth observing that 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 Privacy Act already applies to those organisations.

---

[54] *Privacy Act 1988* (Cth) s 3.
[55] Ibid s 6 (definition of 'APP entity' and 'organisation').
[56] See ibid ss 6 (definition of 'APP entity' and 'organisation'), 6D.
[57] *Privacy Act 1988* (Cth) s 4 (definition of 'APP entity' and 'organisation'). Note that under s 7C political acts and practices connected with the political process, including contractors and volunteers, are also generally exempt.
[58] Attorney General's Department (n 25) 28.
[59] OAIC, *Submission to Privacy Act Review* (n 26) 62.
[60] *Privacy Act 1988* (Cth) s 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.
[61] *Privacy Act 1988* (Cth) s 7B(5).

Protection of 'personal information'

2.2.14 The Tasmanian PIPPs provided for in the PIPA generally apply to the protection of personal information.[62] Personal information is defined in the Act to mean:[63]

> 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.

2.2.15 In the following sections of this Issues Paper, the various elements of this definition will be discussed in detail and compared with other jurisdictions where such comparisons are relevant. A few points of difference are briefly noted.

- The PIPA does not make it clear whether it matters if the information or opinion is true,[64] nor does it make clear whether it matters if the information is recorded in a material form.[65]
- However, the PIPA definition does include information about a person who has been dead for not more than 25 years, which is a shorter period than in some other Australian jurisdictions.[66]

Information or opinion 'about an individual'

2.2.16 The requirement that information be 'about an individual' has been interpreted as requiring that the individual in question is the subject matter of the information or opinion.[67] However, it is uncertain 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.[68]

2.2.17 In contrast, the European Union's *General Data Protection Regulation 2016/679* ('GDPR') defines personal information with a broader scope, by reference to 'any information *relating to* an identified or identifiable natural person'.[69] The Court of Justice of the European Union has made it clear that 'relating to' includes where the data relates to an individual in terms of the content, purpose, or result/effect of the data.[70]

---

[62] 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 [2.2.38]).
[63] PIPA (n 40) s 3 (definition of 'personal information').
[64] 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.'
[65] 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) <https://www.oaic.gov.au/privacy/guidance-and-advice/what-is-personal-information/>.
[66] Cf *Privacy Act 1988* (Cth).
[67] *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFC 4 [63].
[68] See, eg, OAIC, *Submission to Privacy Act Review* (n 26) 27–33. The OAIC recommended that the definition be clarified to include references to inferred information.
[69] GDPR (n 29) (emphasis added).
[70] 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).

Identity is 'reasonably ascertainable'

2.2.18 Personal information can include information which does not name or identify the person directly, but where the person's identity is 'reasonably ascertainable' when combined with other information. There is no definition of 'reasonably ascertainable' in either the PIPA, judicial interpretations, or guidance by the Tasmanian Ombudsman.

2.2.19 The Commonwealth definition of personal information uses the term 'reasonably identifiable'. Guidance from the OAIC emphasises that 'reasonably identifiable' allows reference to:

- the nature and amount of information that might be available;
- the range of persons who might have access to the information in question; and
- the practicality of using that information to identify the individual.[71]

2.2.20 However, it is generally accepted that neither anonymous nor, importantly, pseudonymous data are included in the definition of personal information.[72] Again, in contrast, the Court of Justice of the European Union's interpretation of the 'identifiability' of information appears broader and this is also reflected in the provisions of the Regulation with the specific inclusion of pseudonymous data as personal data in article 4(5) of the GDPR.[73]

2.2.21 No matter how the term is precisely defined, this Issues Paper observes that modern technology may make it easier to draw connections to identity, due to increasingly sophisticated forms of analysis and increased access to other sources of personal information.

De-identification and pseudonymisation

2.2.22 In relation to the ability to identify the individual, the PIPPs also include obligations to permanently de-identify personal information if it is no longer needed for any purpose (PIPP 4(2)) or before disclosing certain health information (PIPP 10(5)). However, it is unclear what extent of de-identification is required—whether it requires that it be no longer technically possible to identify the person at all, or whether it only requires that the identity of the person be no longer 'reasonably ascertainable'.

2.2.23 Under Commonwealth law, personal information is de-identified 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable'.[74] For the purposes of the Privacy Act, de-identified information is no longer 'personal information'. It is therefore generally not subject to the protection of the APPs, even though it may be technically possible to identify the individual concerned, particularly if the information is made available to others or released publicly such as through a data breach.

2.2.24 The possibility of de-identified information being re-identified with the help of additional information is covered in the GDPR. 'Personal data' is defined in the GDPR as 'any information relating to an identified or identifiable natural person ('data subject')'. These regulations adopt a broader approach for whether information is 'identifiable' and therefore protected.

[71] OAIC, *What is Personal Information* (Guidance Document, May 2017) 8.
[72] See Australian Competition and Consumer Commissioner ('ACCC'), *Digital Platforms Inquiry* (Final Report, June 2019) 407, figure 7.11.
[73] For a relevant case see: Case C-582/14, Breyer, ECLI: EU:C:2016:779.
[74] *Privacy Act 1988* (Cth) s 6(1) (definition of 'de-identified').

2.2.25 Relevantly, the GDPR's protective scope covers information which has been subject to 'pseudonymisation', which 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*'.[75] It must be emphasised that pseudonymisation is different from complete anonymity. 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 no longer protected by the GDPR.[76]

2.2.26 The report of the Australian Competition and Consumer Commission's ('ACCC') in the Digital Platforms Inquiry referred to the GDPR in recommending that reform of the Privacy Act should include 'protections or standards for de-identification, anonymisation and pseudonymisation of personal information'. According to the report, this was required in order to 'address the growing risks of reidentification as datasets are combined and data analytics technologies become more advanced'.[77]

2.2.27 The OAIC has also recommended that the Privacy Act be amended to adopt the GDPR references to pseudonymisation and anonymisation. However, the OAIC also recommend (in contrast with the scope of the GDPR) that even anonymised data, which is data that has been stripped of identifying information, should be subject to various obligations under the APPs. These include:

- informing individuals if their data may be anonymised and used for additional purposes;
- reasonably maintaining anonymised data against misuse, loss or unauthorised access; and
- prohibiting entities from re-identifying information collected anonymously.

2.2.28 The OAIC also submitted that individuals should be notified when the privacy of their anonymised personal information has been breached, if this breach creates a risk of re-identification which is likely to result in non-remediable serious harm.[78] The instances in which data breaches must be notified to the individual are discussed further below at [2.4.21]–[2.4.28].

Deceased persons

2.2.29 The PIPA protects the personal information of persons for up to 25 years after their death.[79] Under section 3A, the next of kin is able to exercise the personal information rights of a deceased person, including amending and correcting the personal information in question. This aligns with rights provided by the *Right to Information Act 2009* (Tas).[80]

[75] GDPR (n 29) art 4 (emphasis added). The GDPR does not regulate anonymous information, 'namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable': at recital 26.
[76] GDPR (n 29) recital 26.
[77] ACCC, *Digital Platforms Inquiry* (n 72) 476.
[78] OAIC, *Submission to Privacy Act Review* (n 26) 33–5.
[79] This was introduced in the *Personal Information Protection Amendment Act 2009* (Tas).
[80] 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 (n 40) sch 1.

2.2.30 Privacy legislation in NSW and Victoria similarly protects the personal information of deceased individuals, but for a longer period of not more than 30 years after their death.[81] Recommendations[82] and efforts have been made towards developing a nationally consistent approach towards accessing digital records upon death or incapacity.[83] At a Meeting of Attorneys-General in August 2022 participants agreed on a 'national workplan for consideration of a nationally consistent scheme for access to digital records upon death or loss of decision-making capacity'.[84] Furthermore, the participants agreed to 'provide drafting instructions to the Parliamentary Counsel's Committee (PCC) for the development of uniform model legislation for a national access scheme for digital records after death or incapacity' and noted that 'officials will work with PCC to prepare draft model laws for public consultation in 2023'.[85]

Types of information given additional protection

2.2.31 Within what amounts to 'personal information', the PIPA further distinguishes several categories of information which are subject to greater or lesser protection, including basic, health, sensitive, employee, and law enforcement information. This section discusses information that is granted additional protection.

Sensitive information

2.2.32 Under the PIPA framework, certain categories of personal information are classed as 'sensitive information', defined as:[86]

> '(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;'.

---

[81] 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').

[82] NSW Law Reform Commission, *Access to Digital Records Upon Death or Incapacity* (Report No 147, December 2019) 81–3.

[83] Council of Attorneys-General, *Communique* (27 July 2020) <https://www.ag.gov.au/sites/default/files/2020-07/Council of Attorneys-General communiqué – July 2020.pdf>; Meeting of Attorneys-General, *Communique* (31 March 2021) <https://www.ag.gov.au/about-us/who-we-are/committees-and-councils/meeting-attorneys-general>.

[84] Council of Attorneys-General, *Communique* (12 August 2022) <https://ministers.ag.gov.au/media-centre/meeting-attorneys-general-communique-12-08-2022>.

[85] Council of Attorneys-General, *Communique* (9 December 2022) <https://ministers.ag.gov.au/media-centre/standing-council-attorneys-general-communique-09-12-2022>.

[86] PIPA (n 40) s 3.

2.2.33 The categorisation of personal information as 'sensitive information' generally gives rise to additional requirements under the PIPPs. First, use or disclosure of sensitive information must be *directly* related—rather than related, simpliciter—to the primary purpose for which the information was collected.[87] Second, collecting sensitive information requires the consent of the individual concerned unless the PIPA specifies otherwise. For example, the Act provides exceptions where collection is required or permitted by law, or is necessary to prevent or lessen serious and imminent threat to life or health.[88]

2.2.34 The extent of these obligations and comparisons with other jurisdictions is discussed further below at [2.3].

Health Information

2.2.35 Health information is a type of 'sensitive information'.[89] It is defined in the PIPA by reference to both the nature of the information and where it has been collected. It includes personal information or opinion relating to:[90]

- the health of an individual such as their physical, mental, or psychological health;
- any disability the individual might have had at any time;
- the individual's express wishes for future health provision; and
- any health services that have been provided, or will be provided, to them.

2.2.36 It is unclear why the provision expressly includes both personal information and an *opinion* about a person's health, given that 'personal information' is already defined to include an opinion about an individual.[91]

2.2.37 Health information also includes:[92]

- other personal information collected in providing a health service (defined as an activity where the person performing the activity claims it to affect a person's health; diagnose or treat illness, injury or disability; dispense prescription medication; or provide disability, palliative care, or aged care service);[93]
- 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.

2.2.38 Unlike the first two descriptions of health information, the description of genetic information does not include the term 'personal information'. Therefore, it is unclear whether that aspect of the definition is broader, in the sense that it includes information which is not personal information as defined in the PIPA. 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.

---

[87] Ibid sch 1, PIPP 2(1).
[88] Ibid sch 110.
[89] Ibid s 3 (definition of 'sensitive information', para (b)).
[90] Ibid s 3 (definition of 'health information', para (a)).
[91] Ibid s 3 (definition of 'personal information').
[92] Ibid s 3 (definition of 'health information').
[93] Note that a 'health service' is defined differently in the *Health Complaints Act 1995* (Tas). See discussion below at [4.2].

2.2.39 Given health information is a type of sensitive information, it is subject to various additional protections under the PIPPs. However, there are certain exceptions that apply to health information, but which do not apply to other categories of sensitive information.

2.2.40 For example, health information can be disclosed by a health service to a relative or responsible person where the individual concerned is unable to give or communicate consent.[94] PIPP 10 also allows health information to be collected without the individual's consent for various reasons, including where it is necessary to provide a health service to the individual.

2.2.41 In limited circumstances, health information may also be collected without consent of the individual where it is impracticable to seek such consent.[95] Various requirements must be met for this to be permissible, including that the collection is necessary for:

- 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.

2.2.42 Any health information collected in these limited circumstances must be permanently de-identified before being disclosed.[96] This Issues Paper observes that this requirement may impact the development and use of pseudonymous datasets (discussed above at [2.2.24]–[2.2.27]) for health research that involves comparing the characteristics within a selected sample population.[97]

Biometrics and facial recognition

2.2.43 Biometric information is information relating to the physical characteristics of an individual, such as their face, gait, fingerprints, signature, or voice. Biometrics are commonly used in technology to verify identity, such as through facial recognition or fingerprint sensors on smartphones. Under the PIPA, biometrics are not included as a discrete form of personal information.

2.2.44 In contrast, biometrics are granted additional protection under the Privacy Act. This is achieved through its classification as 'sensitive information'—the Commonwealth definition of the term expressly includes:[98]

- 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.[99]

[94] PIPA (n 40) sch 1, PIPP 2(4).
[95] It must be a situation where it is not possible to use non-identifying information, impracticable to seek the individual's consent, and the collection is done in accordance with law and any professional confidentiality obligations: PIPA (n 40) sch 1, PIPP 10(4).
[96] Ibid sch 1, PIPP 10(5).
[97] Note that the assignment, use, and disclosure of Commonwealth government healthcare identifiers is also regulated under the *Healthcare Identifiers Act 2010* (Cth).
[98] *Privacy Act 1988* (Cth) s 6.
[99] 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.

2.2.45 At the Commonwealth level, The Australian Human Rights Commission have also highlighted the significant privacy risks associated with some uses of biometric technology, including facial recognition technology in surveillance.[100] Drawing from examples in other jurisdictions, including the European Union, the Commission recommended numerous reforms, including the following relevant recommendations:[101]

- Recommendation 19: to create express protections for human rights when facial recognition technology is used in certain types of decision-making. First, in decision-making that impacts a person's legal or similarly significant rights. Second, 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 therefore 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.[102]
- Recommendation 20: to introduce a moratorium on the use of facial recognition technology until the kind of protections discussed in Recommendation 19 are in place.
- Recommendation 21: to introduce a statutory cause of action for invasion of privacy (discussed in detail further below at [4.3]).

2.2.46 The higher privacy risk attached to certain uses of biometric technology was likewise noted by the OAIC in its submission to the review of the Commonwealth Privacy Act. In particular, the OAIC identified activities involving facial recognition as an example of higher privacy risk necessitating greater protections. One way to achieve this is through requiring the entity using the technology to, on request, provide evidence of steps taken to comply with privacy principles.[103]

2.2.47 One example is the Identity-matching Services Bill 2019 (Cth) that aims to facilitate inter-governmental exchange of information across Australia, which means it has a direct impact on Tasmania. The Tasmanian Government has provided information on driver licences to the Commonwealth's National Driver Licence Facial Recognition Solution. However, the data is currently in a segregated partition of the federal system and the Tasmanian government has not permitted that information to be accessed by any other agency or jurisdiction until the Bill has passed.[104]

2.2.48 The sharing of information between government agencies is also discussed next in relation to public information, and generally in Part 3 below.

Information which is less protected by the PIPA

2.2.49 There are various situations where information receives less than the general level of protection. This may be based on the type of information, the context in which it is used, or because legislation otherwise varies the degree of protection provided. The source of the reduced protection can be both within and outside of the PIPA.

2.2.50 First, Division 2 of the PIPA sets out certain bodies or types of information that are subject to fewer obligations or exempted entirely. This includes courts and tribunals as well as various public legal officers, as discussed above at [2.2.2]. Types of information subject to exemptions include basic

[100] Australian Human Rights Commission ('AHRC'), *Human Rights and Technology Final Report* (Final Report, 2021) ch 9.
[101] Ibid 116–23.
[102] Ibid 117, 119 (referring the example raised in the report).
[103] See, eg, OAIC, *Submission to Privacy Act Review* (n 26) [7.17], [7.34].
[104] See Tasmania, *Parliamentary Debates*, Legislative Council, 24 August 2021, 27–8.

personal information, employee information, public information, and law enforcement information, each of which are discussed in this section.

2.2.51 Second, there are also provisions in the PIPA that allow the Minister to grant exemptions for any or all provisions of the Act if the Minister determines this to be in the public benefit. Emergency declarations at the Commonwealth level can also have a similar effect in operation. These provisions are also discussed in this section.

2.2.52 Third, many of the PIPPs set out in Schedule 1 of the PIPA include exceptions relating to the handling of information in a way authorised by law, including by other legislation ancillary to the PIPA. These exceptions are discussed in Part 3 below when each of the PIPPs are considered in detail.

Basic personal information

2.2.53 'Basic personal information' means the name, residential address, postal address, date of birth and gender of an individual.[105]

2.2.54 Public authorities are able to use basic personal information without the person's consent and for purposes that were not the primary purposes for collecting the information. Basic personal information can also be shared with other 'public sector bodies'. The use or disclosure must only be reasonably necessary for the efficient storage and use of that information.[106]

2.2.55 However, two points are unclear. The first is whether reasonable necessity is judged from the view of the public authority that initially *collected* the information or from the view of the public sector body with which the information is *shared*. The second is whether use of the term 'public sector bodies' rather than 'public authorities' means that basic personal information can be shared with entities who are not subject to the PIPPs and who may otherwise lawfully make use of the information shared. Under the PIPA, the term 'public authority' (discussed above at [2.2.1]) is defined and included in the list of bodies that may constitute a personal information custodian. However, the term 'public sector body' is not so defined.

Employee information

2.2.56 Employee information is defined inclusively as personal information about an individual relating to their current, past, or prospective employment.[107] While included under the PIPA as a form of personal information,[108] it is accorded distinct treatment.

2.2.57 Specifically, a number of PIPPs do not apply to employee information, as follows:[109]

- Collection—employee information about an individual need not be collected from that individual and the individual need not be informed that the information has been collected (PIPP 1(4) and (5)).
- Use of unique identifiers—unique identifiers for individuals can be assigned, adopted, used or disclosed, or required without complying with the requirements of PIPP 7.

[105] PIPA (n 40) s 3 (definition of 'basic information').
[106] Ibid s 12.
[107] This includes information about their selection, employment, training, discipline or resignation, termination, conditions of employment, 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: see ibid s 3 (definition of 'employee information').
[108] PIPA s 3 (definition of 'employee information').
[109] Ibid s 10.

- Sensitive information—to the extent that the employee information includes sensitive information that would otherwise be subject to additional protections under PIPP 10, these additional protections do not apply.

2.2.58 Employee information is also treated differently in PIPP 2, relating to use of personal information. While personal information can generally only be used and disclosed for the purpose for which it was collected, an express exception allows employee information to be used to assess a person's suitability for appointment or employment.[110] Employee information can also be shared with other bodies subject to the PIPA, but only where the information will be used as employee information.[111] Otherwise, the standard restrictions on sharing information apply.

2.2.59 The Commonwealth Privacy Act also generally exempts the handling of employee records[112] and information relating to the employment relationship.[113] The Privacy Act review has questioned whether employee information is adequately protected and whether some of the APPs should apply to some or all employee records.[114] In its submission, the OAIC recommended that the exemption for employee records be removed subject to an appropriate transition period.[115]

Public information

2.2.60 Public information is defined as 'any personal information that is: (a) contained in a publicly available record or publication; or (b) taken to be public information under any Act'.[116] The PIPA does not apply to public information.[117]

2.2.61 By not protecting publicly available information in this way, the PIPA operates in a similar way to privacy legislation in various other jurisdictions, including NSW,[118] Victoria[119] and Queensland.[120] In contrast, federal legislation (the Privacy Act) does not have a general exemption that removes protections for publicly available information.

Law Enforcement Information

2.2.62 In the PIPA, 'law enforcement information' includes information reasonably likely to:

- prejudice investigation of a breach or enforcement of the law;
- disclose confidential sources;
- prejudice the effectiveness of methods or procedures relating to breaches of the law;
- endanger life or safety or increase the likelihood of harassment or discrimination; or
- disclose information collected for intelligence including criminal databases.

[110] Ibid sch 1, PIPP 2(1)(i).
[111] Ibid 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.
[112] 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')
[113] Ibid 7B(3).
[114] Attorney-General's Department (n 25) 32.
[115] OAIC, *Submission to Privacy Act Review* (n 26) 64.
[116] PIPA (n 40) s 3.
[117] Ibid s 8.
[118] *Privacy and Personal Information Protection Act 1998* (NSW) s 4(3)(b).
[119] *Privacy and Data Protection Act 2014* (Vic) s 12.
[120] *Information Privacy Act 2009* (Qld) sch 1 cl 7(a).

2.2.63 In some cases, 'law enforcement information' also extends to information that may reveal unlawful behaviour by law enforcement bodies, such as information that reveals the use of illegal methods to investigate a crime. However, such information will only be included in the definition—and therefore exempt from compliance with certain PIPPs—if disclosure of the information is *not* in the public interest.[121]

2.2.64 Whether disclosure of information is or is not in the public interest is determined by reference to a non-exhaustive list of matters set out in the *Right to Information Act 2009* (Tas). For example, whether disclosure would enhance scrutiny of government action and whether it would promote or harm the administration of justice.[122]

2.2.65 Under the PIPA, law enforcement information is exempt from several PIPPs in certain circumstances where the law enforcement agency considers exemption appropriate.[123] Specifically, where it 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.[124]

2.2.66 'Law enforcement agency' covers a wide variety of bodies involved with law enforcement. Among others, this includes police forces (of the Commonwealth, 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.[125]

2.2.67 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.[126]

2.2.68 Other state jurisdictions also provide exemptions for law enforcement agencies and activities, including NSW, Victoria, and Queensland.[127] In contrast, in the Commonwealth jurisdiction, the Privacy Act does not have a general exemption for law enforcement activities. However, if other legislation authorises certain activities, and compliance with privacy obligations would impede the ability to effectively carry out such lawful activities, this may limit the operation of some of the federal privacy principles (the APPs).

Public benefit exemptions

2.2.69 Personal information custodians can apply to the Minister for an exemption. The exemption may relate to any or all provisions of the PIPA, and may allow a custodian to deal with personal information in a way not otherwise permitted by the PIPPs. The application must specify the matters

[121] *Right to Information Act 2009* (Tas) s 30(2).
[122] Ibid sch 1.
[123] 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).
[124] PIPA (n 40) s 9.
[125] Ibid s 3 (definition of 'law enforcement agency').
[126] Ibid sch 1, PIPP 2(1)(g).
[127] 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.

listed in section 13, including the provisions of the Act for which an exemption is being sought, the information that the application relates to, and reasons for seeking an exemption.[128]

2.2.70 Whether or not the exemption is granted is based on a balance of public benefit.[129] The Minister may approve an application 'if satisfied that the public benefit [of an exemption] outweighs to a substantial degree the public benefit from compliance with the personal information protection principles'.[130] This may be subject to conditions, if the Minister considers it appropriate. Otherwise, if not satisfied about the balance of public benefit, the Minister may refuse to grant the exemption.

2.2.71 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.[131] 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.

2.2.72 Any determination (whether an approval or a refusal) or revocation has to be published in the Gazette.[132] While the Gazette can be searched by the public, it is not possible to limit the search to only where an exemption has been granted. There is also no easily accessible list of exemptions currently in operation. An examination of the Gazette suggests there have been 11 public benefit exemptions published between 2008 and 2020 as follows: two in April 2011, one in February 2019, and eight in November 2020.[133] As an example, on 25 November 2020, exemptions were gazetted for information relevant to a civil claim against the State of Tasmania and held by nine government departments.[134]

2.2.73 Other Australian jurisdictions such as NSW,[135] Victoria,[136] and Queensland[137] also provide for similar exemptions on the basis of the public interest. The respective parliaments in the latter two jurisdictions, also have the power to disallow an exemption.[138]

2.2.74 The Commonwealth Privacy Act also provides for public interest determinations which excuse breaches of privacy, either where it may occur in the future or *after* they have already occurred. Where an entity's acts or practices may breach, or have breached, a privacy obligation, the OAIC may make a public interest determination if it is satisfied that the public interest in the act or practice substantially outweighs the public interest in adhering to the privacy obligation.[139] 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.[140]

2.2.75 The Australian Information Commissioner may make a determination that applies to all entities subject to the APPs. The mechanisms for relevant processes are set out in the Privacy Act.[141] Where an urgent decision is needed, the Act also allows the Minister to make a temporary

[128] PIPA (n 40) s 13.
[129] Ibid s 14.
[130] Ibid.
[131] Ibid s 15.
[132] Ibid ss 14(3), 15(2).
[133] The Tasmanian Government Gazette is available at <http://www.gazette.tas.gov.au/editions>.
[134] Tasmania, *Gazette*, No 22037, 25 November 2020 <http://www.gazette.tas.gov.au/editions/2020/november_2020/22037_-_Gazette_25_November_2020.pdf>.
[135] *Privacy and Personal Information Protection Act 1988* (NSW) s 41.
[136] *Information Privacy Act 2009* (Qld) s 157.
[137] Although principles relating to Data Security and Access and Correction cannot be disapplied: ibid s 29(3).
[138] See, eg, *Privacy and Data Protection Act 2014* (Vic) s 42.
[139] *Privacy Act 1988* (Cth) s 72.
[140] Ibid s 80B.
[141] Ibid ss 74–9.

determination,[142] including on the Commissioner's own initiative (without an application).[143] The OAIC maintains a register of public interest determinations.[144] There have been eight since 2015, with five currently in effect.

Emergency declarations

2.2.76 The Tasmanian PIPA does not expressly provide any general exceptions relating to responding to emergency situations. However, this situation is addressed under federal law.

2.2.77 Part VIA of the Commonwealth 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. This includes allowing all entities subject to the Commonwealth APPs to handle personal information without the consent of the person concerned. Entities are also protected against breaches of secrecy provisions in other legislation and obligations of confidence that exist in general law.[145] An example of a recent declaration was in January 2020 to respond to that summer's bushfire crisis.[146]

2.2.78 The Royal Commission into National Natural Disaster Arrangements recommended that all Australian governments should ensure that personal information of individuals affected by a natural disaster is able to be appropriately shared between all levels of government, agencies, insurers, charities, and organisations delivering recovery services. However, this must account for all necessary safeguards to ensure the sharing is only for recovery purposes.[147]

Questions:	
2.1	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'?
2.2	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?
2.3	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?
2.4	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?
2.5	Are the other categories of information, including health and other forms of sensitive information suitable?
2.6	Are the exceptions, including the process for declaring and publishing public benefit exemptions, suitable?

[142] Ibid s 80A.
[143] Ibid s 80A(2).
[144] Ibid s 80E.
[145] Ibid s 80P.
[146] OAIC, *Submission to Privacy Act Review* (n 26) 47.
[147] Australian Government, *The Royal Commission into National Natural Disaster Arrangements Report* (Report, 2020) recommendation 22.2.

2.3 Personal Information Protection Principles

The PIPPs in comparison with other jurisdictions

2.3.1 The PIPA sets out ten Personal Information Privacy Principles ('PIPPs'). Each is considered in turn below. As discussed above at [2.2.9]–[2.2.13], the APPs (Australian Privacy Principles) under the Commonwealth Privacy Act were developed with the intention that they could serve as a model for other Australian jurisdictions to follow. Given the importance of consistency across Australian jurisdictions as a potentially useful aim for any reform to privacy laws in Tasmania, the Commonwealth APPs are presented as a point of comparison and, where relevant, any substantial differences with privacy legislation in other states or territories are also noted.

Collection

2.3.2 Under Tasmanian law, PIPP 1 restricts the collection of personal information. It requires that the collection is by lawful means, is necessary for one or more of the custodian's functions or activities, and that notice is given to the person whose information is involved.[148] The PIPA does not define how a custodian's functions or activities are determined.

2.3.3 Under the Commonwealth Privacy Act, APP 3 governs the collection of solicited personal information. Under APP 3, government agencies can collect personal information in two scenarios. First, where it is *reasonably* necessary for one or more of the agency's functions, taking into account how it impacts the person affected. Alternatively, where the information is *directly related to* one or more of the agency's functions.[149] Guidance on APP 3 notes that such functions are identified through reference to the legal instruments which confer or describe the agency's functions.[150] Activities must be incidental or otherwise closely related to those functions.

2.3.4 The PIPA provides for the collection of personal information where necessary, while APP 3 includes the requirement of reasonableness in considering what is necessary. Further, the PIPA mandates collection by lawful means, whereas APP 3 requires that any collection must be by both lawful *and fair* means, which may preclude intimidation, deception, or unreasonably intrusive measures—even if they are technically lawful.[151]

2.3.5 Regarding notice, APP 5 on notification of the collection of personal information, requires that notice of the circumstances of the collection must be provided prior to collection, unless it is not practicable to inform them before or during collection.

2.3.6 APP 5 further requires entities to disclose who else may have access to the information once it is collected, including overseas recipients. It also requires entities to provide information in their privacy policy on how to complain about a breach of the privacy principles. There is no equivalent provision for these two requirements in the Tasmanian PIPA.

[148] PIPP 1 requires a custodian to only collect personal information where it is necessary for one of its functions or activities. Personal information can only be collected by lawful means—a term not defined in the Act. The individual concerned must be made aware of various information, including who the custodian is, that the individual has a right of access to the information, the purposes for which the information is collected, the intended recipients of the information, any law that requires collection, and the consequences if information is not provided. If it is reasonable and practicable to do so, personal information must be collected from the individual concerned. Otherwise, the custodian must take reasonable steps to inform the individual of the circumstances of collection unless doing so would pose a serious threat to the life, safety, health, or welfare of any individual.

[149] See OAIC, *Australian Privacy Principles Guidelines* (Guidance Document, July 2019) ch 3 [3.62].

[150] Ibid [3.10]–[3.12]. 'Legal instruments' are not limited to legislation, but also extends to executive schemes or arrangements.

[151] See ibid [3.62].

2.3.7 The Privacy Act also allows for collection of health information in 'permitted health situations', meaning where the information is necessary to provide a health service, and required or authorised under Australian law or in accordance with rules of health or medical bodies that deal with obligations of professional confidentiality.[152]

2.3.8 On the source of the information, PIPP 1 requires information to be collected from the person concerned where it is reasonable and practicable to do so. If this is not possible and information is collected from someone else, reasonable steps must be taken to notify the individual that their information has been collected, unless this would seriously threaten anyone's life, safety, health, or welfare.[153]

2.3.9 APP 3 similarly permits information to be collected from someone other than the person concerned. Further, APP 3 provides two additional situations where this is permissible: where the individual concerned has consented; or where the entity is required by law to do so.

2.3.10 Where personal information is not collected directly from the individual concerned, the OAIC recommended that an obligation be placed on entities to take reasonable steps to satisfy themselves that the initial collection was compliant with privacy obligations. For example, that the information was initially collected using means that were lawful and—in the case of the APPs—fair.[154]

Use and disclosure

2.3.11 Under Tasmanian law, PIPP 2 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 ('primary purpose'). Otherwise, it can be used or disclosed for another purpose ('secondary purpose')[155] only if it satisfies one of the other permissible circumstances listed in PIPP 2.[156]

2.3.12 One example is where the law requires or authorises the use or disclosure.[157] However, it is not clear how far this authorisation extends, including whether it is limited to legislation or whether it would also include statutory instruments or contractual obligations created by the custodian themselves. In guidelines for the Commonwealth Privacy Act,[158] the OAIC indicated that 'required' means an entity has no choice but to use or disclose the information. Meanwhile, 'authorised' means the entity is permitted, but not required, to do so. However, it is generally not sufficient for there to be

[152] *Privacy Act 1988* (Cth) s 16B.
[153] PIPA (n 40) sch 1, PIPP 1(4)–(5).
[154] OAIC, *Submission to Privacy Act Review* (n 26) 44 (recommendation 17).
[155] 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).
[156] The permitted purposes under PIPP 2 include:

- the purpose of the use or disclosure is related (or if sensitive information—directly related) to the primary purpose and the individual would reasonably expect use or disclosure for that purpose;
- the individual has consented;
- the information is de-identified, use or disclosure is necessary for research or statistical analysis in the public interest, and it is impracticable to seek prior consent or the recipient is reasonably believed to be not likely to disclose the information;
- it 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;
- it is a necessary part of an investigation by the custodian or report to relevant authorities of suspected unlawful activity;
- it is required or authorised by or under law;
- believed to be 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;
- it has been requested by Commonwealth security agencies; and
- it is to be used as employee information or transferred to another custodian for such use.

[157] PIPA (n 40) sch 1, PIPP 2(1)(f).
[158] OAIC, *Australian Privacy Principle Guidelines* (n 149) ch B.

merely a *lack* of prohibition on use or disclosure, or for there to be a general or incidental authority. For example, if an entity is conferred a general authority to create statutory instruments or otherwise do anything necessary or convenient in carrying out its functions, this would not be interpreted as allowing an agency to create the authority to use or disclose personal information. The Privacy Act also does not extend protection to contractual obligations.

2.3.13 Another example where information can be used or disclosed for a secondary purpose is where the information is 'basic information'. As discussed above at [2.2.54], public authorities can share 'basic information' with another public sector body where this 'is reasonably necessary for the efficient storage and use of that information'.[159]

2.3.14 In the context of healthcare, under Tasmanian law, PIPP 2 makes explicit provision for health service providers to disclose an individual's health information to another person who is responsible for that individual in certain circumstances.[160] This covers where 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 it is not contrary to the wishes of the individual.

2.3.15 Under Commonwealth law, APP 6 generally restricts the use or disclosure of personal to where such use or disclosure is for a primary purpose. However, there are a few differences between Commonwealth and Tasmanian laws.

2.3.16 First, the Commonwealth Privacy Act contains guidelines on use and disclosure of certain types of information that are not provided for in the Tasmanian PIPA. These are:

- Biometric information or biometric templates can be disclosed to enforcement bodies but only in compliance with guidelines issued by the Australian Information Commissioner.
- Genetic information can be used or disclosed in accordance with guidelines under the Privacy Act if the use or disclosure is done to lessen or prevent serious threat to life, health or safety of a genetic relative.

2.3.17 Second, there are discrepancies between the Commonwealth and Tasmanian Acts regarding the list of circumstances where information can be used or disclosed for a secondary purpose. Some circumstances in the Privacy Act do not have equivalents under the PIPA. This includes where disclosure is reasonably necessary for a confidential alternative dispute resolution process.[161]

2.3.18 Third, conversely, some circumstances provided for in the PIPA do not have equivalents under the Privacy Act. This includes, for example:

- use and disclosure for research and statistical analysis generally (note, however, that the Commonwealth law does make special provision for health information, which may be used or disclosed where necessary for research or analysis relevant to public health or safety, provided certain criteria are satisfied);[162] and
- use of information as employee information to assess whether an individual is suitable to be appointed or to continue their employment.

[159] PIPA (n 40) s 12.
[160] PIPP 2(5) sets out when a person is responsible for another.
[161] 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 of Australia such as war or warlike operations, peacekeeping or peace enforcement or civil aid, humanitarian assistance, medical or civil emergency or disaster relief: *Privacy Act 1988* (Cth) s 16A.
[162] This applies where it is impracticable to obtain an individual's consent, use or disclosure is conducted in accordance with guidelines issued under the Act, and there is reasonable belief that the recipient will not disclose the information: *Privacy Act 1988* (Cth) s 16B.

Data quality

2.3.19 Under Tasmanian law, PIPP 3 requires that a custodian must take reasonable steps to ensure that, having regard to the purpose for which the personal information is to be used, the personal information it collects, uses, holds or discloses is accurate, complete, up-to-date and relevant to its functions or activities.

2.3.20 This is equivalent to APP 10 under Commonwealth law on the quality of personal information.

Data security

2.3.21 Under Tasmanian law, PIPP 4 requires that a custodian must take reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification, or disclosure. Personal information must be destroyed or permanently de-identified if it is no longer needed for any purpose, subject to any necessary approval under the *Archives Act 1983* (Tas).

2.3.22 Under Commonwealth law, APP 11 on the security of personal information also provides similar security obligations. The obligation 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 if the information is not contained in a Commonwealth record or required under an Australian law or court/tribunal order to be retained.

2.3.23 For this privacy principle, the GDPR serves as a useful further point of comparison because it provides greater detail. Australian laws simply require the entities to take 'reasonable steps' to protect the security of personal information. However, 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 [2.2.25]) 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.

2.3.24 The GDPR also allows entities to demonstrate compliance through adherence to an approved code of conduct or certification scheme.

Openness

2.3.25 Under Tasmanian law, PIPP 5 specifies that custodians must document their policies on managing personal information and make these policies available to anyone on request. Custodians must also advise on the sort of information held, why it is held, as well as how it is collected, held, used, and disclosed.

2.3.26 Under Commonwealth law, APP 1 on the open and transparent management of personal information provides for similar requirements. It requires that policies on the management of personal information must be proactively made publicly available free of charge, usually on the entity's website, as well as upon request and in the form requested.

2.3.27 Compared to the requirements under PIPP 5, APP 1 is more onerous in requiring that an entity's privacy policy also contain information on:

- the purposes for which information is collected, used and disclosed;

- how an individual may access their personal information and have it corrected;
- how an individual may complain about a privacy breach; and
- whether the entity is likely to disclose personal information to overseas recipients, and if yes, where such recipients are likely to be located.

2.3.28 In addition, APP 1(2) requires 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 APP 1(2), the OAIC developed the *Privacy (Australian Government Agencies – Governance) APP Code 2017*.[163] This is registered under the Privacy Act as an 'APP code'—a code of practice that sets out how one or more APPs are to be complied with, and which has the same legally binding effect as the APPs themselves.

2.3.29 The code establishes various measures that agencies must put in place in order to comply with APP 1(2). This includes for agencies 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, and to make the assessment publicly available and listed on a publicly available register.

Access and correction

2.3.30 Under Tasmanian law, PIPP 6 allows a custodian to provide access to personal information it holds upon request from the person concerned, or else to provide access under section 13 of the *Right to Information Act 2009* (Tas) as if the custodian were bound by that Act. PIPP 6(2) also allows an individual to request their information be amended if it is incorrect, incomplete, out of date, or misleading. Part 3A of the PIPA provides further details, including what form the request must be in, what information it must contain, and what must be done if a custodian refuses the request.[164]

2.3.31 Under Commonwealth law, APP 12 on access to personal information and APP 13 on correction of personal information make similar provisions. However, there are some differences from PIPP 6 in relation to time limits, allowing access to information, bases for correction, and notifying third parties of corrections, as outlined below.

- Time limits: under APPs 12 and 13, requests to access or correct personal information must be handled within 30 days and reasons must be given for any refusal, whereas under PIPP 6, the time limit is 20 working days.[165]

[163] 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/>.

[164] Under Part 3A, a person can request amendment of their personal information held by a custodian where it is incorrect, incomplete, out of date, or misleading. The custodian can either correct the information or add an appropriate notation, but any amendment must not delete information or destroy the document unless the State Archivist agrees. The custodian must decide on whether to correct the information within 20 working days, and provide reasons for any refusal. If correction is refused, the person can require a notification of the claimed errors be added and that any disclosure of the information includes a statement concerning the notation.

[165] PIPA (n 40) s 17E.

- Allowing access: under APP 12, if the request for how to access personal information is reasonable and practicable to fulfil, it should be accepted, whereas under the PIPA there is no analogous obligation to allow access.
- Access charge: the Commonwealth Privacy Act expressly provides that an agency cannot charge an individual for access to their information.[166]
- Grounds for correction: under APP 13, as well as the grounds provided under PIPP 6, there is an additional ground allowing information to be corrected where it is irrelevant. Relevance is considered by the entity holding the information, from the perspective of *the purpose for which the information is held*.[167]
- Notice to third parties: under APP 13, in circumstances where an individual's personal information has been disclosed by one entity to another entity, the individual can request that the entity notify the other entity of the correction. Reasonable steps must be taken to comply with this request unless doing so would be impracticable or unlawful.[168] PIPP 6 does not contain an analogous ability.

2.3.32 Only personal information that the custodian 'holds' may be accessed and corrected. This means that information published on social media falls outside of the operation of PIPP 6. As the OAIC has noted, such information is no longer within an agency's possession or control and is therefore not 'held' by that agency. The OAIC has recommended that the obligation to correct personal information should extend to taking steps to correct publicly available information that has been posted online.[169]

2.3.33 The approach can be seen in the GDPR, where the right to rectify inaccurate data applies even where the 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.

Unique identifiers

2.3.34 An 'identifier' is anything a personal information custodian assigns to an individual to identify them for the purposes of the custodian's operations. It could be a number, letter, symbol, or a combination of these. However, the definition explicitly clarifies that an individual's name or an Australian Business Number are *not* identifiers.[170]

2.3.35 Under Tasmanian law, PIPP 7 restricts the use of unique identifiers. It prevents a custodian assigning a unique identifier to an individual unless it is necessary to carry out any of its functions efficiently.[171] The custodian also cannot adopt unique identifiers assigned by other custodians unless necessary to carry out its functions, the individual has consented, or it is to perform a contractual obligation to that custodian. A custodian cannot use or disclose a unique identifier assigned by another custodian unless necessary to fulfil functions to that other custodian or the custodian complies with its obligations under PIPP 2(1) relating to use and disclosure of personal information.

2.3.36 In contrast, under Commonwealth law, APP 9 on the adoption, use, or disclosure of government-related identifiers only restricts the use of such identifiers by *non-government*

[166] 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.
[167] *Privacy Act 1988* (Cth) sch 1, APP 13.1(a).
[168] Ibid sch 1, APP 13.2.
[169] OAIC, *Submission to Privacy Act Review* (n 26) 51.
[170] PIPA (n 40) s 3.
[171] For a discussion of how to identify a custodian's functions, see the discussion in relation to PIPP 1 above at [2.3.2]–[2.3.10].

organisations. Generally, government-related identifiers cannot be adopted by non-government organisations unless authorised by law,[172] and cannot be used or disclosed unless it is:

- reasonably necessary to verify identification for the purposes of its activities or functions;
- done in order to fulfill obligations to state or territory authorities;
- required under law or a court or tribunal order;
- a situation that constitutes a 'permitted general situation' where information or identifiers can be used or disclosed;[173] or
- reasonably believed to be necessary for an enforcement activity conducted by or on behalf of an enforcement body.

2.3.37 In contrast to the rules restricting the use of identifiers by non-government organisations, the use of identifiers by *government* organisations are generally subject to the APPs only where identifiers amount to personal information.

Anonymity

2.3.38 Under Tasmanian law, PIPP 8 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'.

2.3.39 Under Commonwealth law, APP 2 on anonymity and pseudonymity adds the option of using a pseudonym. This may extend the range of lawful and practicable options available to individuals seeking to avoid identification. However, as discussed above at [2.2.23] regarding de-identification, pseudonymous information may no longer be considered 'personal information', since the identity of an individual is no longer apparent or reasonably ascertainable. If this is the case, then it will no longer be protected under the *Privacy Act* or the PIPA.

Disclosure of information outside Tasmania

2.3.40 Under Tasmanian law, in addition to the general limits on disclosure contained in PIPP 2, further restrictions, contained within PIPP 9, apply if the disclosure is to anyone outside of Tasmania.[174]

2.3.41 Under Commonwealth law, APP 8 governs cross-border disclosure of personal information. Compared to PIPP 9, APP 8 allows cross-border disclosure in a broader range of circumstances. An agency can disclose information reasonably necessary for its enforcement activities or where the disclosure is otherwise generally permitted.[175]

---

[172] For a discussion of this term, see the discussion above in relation to PIPP 2 at [2.3.11]–[2.3.18].

[173] 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.

[174] Disclosure is not permitted unless:

- the custodian reasonably believes that the recipient is subject to binding principles substantially similar to the PIPPs;
- the individual concerned consents or the disclosure is necessary for the performance of a contract with the individual or in their interest;
- the custodian has taken reasonable steps to ensure the recipient deals with the information consistently with the PIPPs; or
- the disclosure is authorised or required by any other law.

[175] 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.

2.3.42 However, in other ways, APP 8 is more restrictive. For example:

- Both PIPP 9 and APP 8 allow disclosure where there is a reasonable belief that the recipient is subject to privacy obligations substantially similar to those in Australia. However, APP 8 additionally requires there to be mechanisms for the individual to enforce that protection.
- Both PIPP 9 and APP 8 allow an individual to consent to overseas 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 no longer obliged to take reasonable steps to ensure the overseas recipient does not breach the APPs.
- APP 8 does not make any provision for overseas disclosure to perform certain contracts. In contrast, PIPP 9 allows such disclosure for the purposes of performing a contract between the individual and the custodian, or for concluding or performing a contract between the custodian and a third party that was made in the individual's interests.[176]

2.3.43 The Commonwealth and Tasmanian Acts and their respective principles also differ on who retains responsibility for breaches of privacy principles by the overseas recipients. Both PIPP 9 and APP 8 allow overseas disclosures of personal information on the basis that the Australian custodian or entity has taken reasonable steps to ensure the overseas recipient does not breach the respective privacy principles that apply. Under the PIPA, a custodian is no longer responsible once it has taken reasonable steps. In contrast, under the Privacy Act, the entity retains responsibility.[177]

Sensitive information

2.3.44 As discussed above under [2.2.31]–[2.2.48], sensitive information is a subset of personal information involving an individual's innate characteristics, beliefs, or practices. Health information is a form of sensitive information that relates to the health of an individual or to health services that have been provided to them.

2.3.45 Under Tasmanian law, PIPP 10 augments the protection of personal information provided by the other PIPPs by placing more onerous restrictions on the collection of sensitive information generally.[178] There are also a few additional circumstances in which health information, as a particular type of sensitive information, can be collected.[179]

---

[176] Though there is allowance for authorisation under an international agreement relating to information sharing: see ibid sch 1, APP 8(2)(e)).

[177] *Privacy Act 1988* (Cth) s 16C.

[178] The permitted bases on which sensitive information can be collected are either:

- the individual concerned has consented;
- the collection is required by law;
- the collection is necessary for life and health of any individual and the individual concerned cannot consent, communicate consent or is subject to a guardianship or mental health order;
- the collection is necessary for a legal or equitable claim;
- the sensitive information is collected from members of a non-profit custodians which have only racial, ethnic, political, religious, philosophical, professional, trade or trade union aims where the custodian has undertaken not to disclose that information without consent;
- the collection is necessary for research or statistical analysis in the public interest and any resulting publication is de-identified, or where racial or ethnic information is collected for the purpose of welfare or educational services funded by the government. There has to be no practical alternative to collecting the information for these purposes and it is impracticable to seek the individual's consent.

[179] In addition to the circumstances in which sensitive information can be collected, health information can be collected either:

- where the collection 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;
- 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

2.3.46 As well as PIPP 10, which is dedicated to this subset of information, sensitive information is also given increased protection in other PIPPs. For example, PIPP 2 requires that personal information be used or disclosed only for the primary purpose for which it was collected. An exception to this is where a secondary purpose for use or disclosure is 'related' to the primary purpose and the individual would reasonably expect the custodian to use or disclose the information for that secondary purpose. However, if the information in question is sensitive information, the secondary purpose must not only be related, but rather be '*directly* related' to the primary purpose.[180]

2.3.47 Under Commonwealth law, APP 3 on collection of information similarly provides special protections for sensitive information. However, there are differences between PIPP 10 and APP 3 in the exceptions that outline when sensitive information can nevertheless be collected.

- Under PIPP 10, consent of the individual is an exception. Under APP 3, consent on its own is insufficient and the collection of the information must still be reasonably necessary or directly related to one or more of the agency's functions or activities.
- Both PIPP 10 and APP 3 allow for health information to be collected for research purposes. Numerous requirements must be met, including that there are rules governing the collection. Under PIPP 10, the collection must either be required by law (other than the PIPA), or it is done in accordance with professional confidentiality rules set by the relevant health/medical associations. APP 3 specifies the same two authorisation requirements as well as an additional requirement not present in the PIPA: it must be collected in accordance with relevant guidelines approved by the Information Commissioner.[181]
- APP 3 permits sensitive information to be collected for the purposes of a confidential alternative dispute resolution process.[182] No equivalent exception appears in the PIPA's principles.

2.3.48 One point of uncertainty to note regarding PIPP 10 is what it means for collection to be 'required or permitted by law'. Specifically, it is unclear whether and how this differs from the general requirement that personal information must be collected by lawful means,[183] or how it differs, if at all, from other references in the PIPPs to the handling of personal information in a way required or authorised by law.[184]

Other differences between the PIPPs and APPs

2.3.49 In addition to the differences between the PIPPs and the APPs discussed above, a major discrepancy is that there are no PIPPs under Tasmanian law equivalent to APP 4 under Commonwealth law on dealing with unsolicited personal information and APP 7 on direct marketing.

information is collected as required by law or in accordance with professional obligations of confidentiality (such information collected for this purposes must be permanently de-identified before disclosure); or

- 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.

[180] PIPA (n 40) sch 1, PIPP 2(1)(a).
[181] *Privacy Act 1988* (Cth) ss 16B(2)(a), (d)(i)–(iii). See also s 95A, which provides rules around these guidelines.
[182] See ibid s 16A, sch 1 pt 2 APP 3.
[183] See PIPA (n 40) sch 1, PIPP 1(2), 7(4)(a), 9(e). For a discussion of the meaning of required or authorised, see above at [2.3.12].
[184] Ibid sch 1, PIPP 2(1)(f).

Unsolicited personal information

2.3.50 Under Commonwealth law, APP 4 concerns the scenario where an entity receives personal information that it did not request. If this occurs, the entity must determine within a reasonable period whether it *could have* collected the information under APP 3.[185] Generally, if the entity would not have been allowed to collect the information, then the information must be destroyed as soon as practicable unless it would be unlawful to do so. However, if the information can be kept, the other APPs will apply, including obligations to notify the individuals concerned.

2.3.51 In contrast, under Tasmanian law, the PIPA expressly clarifies that PIPP 1 on collection of information does not apply to unsolicited information received by a custodian.[186]

2.3.52 The PIPA does not define 'unsolicited information' and there is no apparent requirement that the unsolicited information must have been sent to the custodian by the individual concerned. The practical effect of this is that a custodian can continue to use unsolicited information, even in circumstances where it could not have collected it directly and where the individual does not know the custodian has the information. As PIPP 1 does not apply, there is no legal requirement to inform the individual concerned that the custodian now has their personal information.

2.3.53 The other PIPPs, namely 2–10, by default apply to unsolicited information. However, of these, PIPPs 2, 3 and 10 concentrate on the *purpose of collection* to assess permissibility. Consequently, it is unclear how they would apply to unsolicited information—precisely because no objective purpose of collection exists. Further, other APPs (and their Tasmanian analogues) generally offer more limited protections than those provided in APP 4. For example, there is no general obligation under the Tasmanian PIPPs to destroy or de-identify the information.[187]

Direct marketing

2.3.54 Under Commonwealth law, APP 7 governs the use or disclosure of personal information for direct marketing—marketing that involves targeting and communicating with individual consumers directly, such as through telemarketing or mail. Direct marketing can be contrasted with marketing done through third parties, such as through advertising media on TV or webpages.

2.3.55 APP 7 imposes obligations on non-government organisations in relation to direct marketing. It does not apply to government agencies, except in limited circumstances where they are engaging in commercial activities.[188]

2.3.56 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.

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

---

[185] APP 3 includes requirements that the information is reasonably necessary for, or directly related to, one or more of the entity's functions, and that any individual whose sensitive information is included in the information provided has consented or an exception applies.

[186] PIPA (n 40) s 11.

[187] PIPP 4 provides for destruction or de-identification only where the information is no longer needed for any purpose: PIPA (n 40) sch 1.

[188] 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.

2.3.58 Under Tasmanian law, the PIPA does not have an equivalent to APP 7. Therefore, while non-government contractors and their sub-contractors must comply with the PIPPs, they are not subject to additional restrictions regarding the use of personal information for direct marketing purposes. As long as 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.

2.3.59 The OAIC recommended that APP 7 be repealed and replaced with a new 'right to object', discussed below at [2.3.76]–[2.3.80]. This right would entitle individuals to object to the use of their personal information for certain purposes, including direct marketing purposes.[189] This recommendation takes inspiration from the GDPR, which provides for this right.

Potential reforms

Notice and consent requirements

2.3.60 Under Tasmanian law, various PIPPs allow the handling of personal information based on the provision of notice to the individual concerned and their consent. Regarding notice, PIPP 1 generally requires various forms of information to be disclosed upon collection, while PIPP 5 requires personal information custodians to clearly set out privacy policies and provide them on request and to respond to requests for advice related to personal information that is collected, held, used and disclosed. 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. However, the PIPA does not define what amounts to 'consent'.

2.3.61 Consent plays a similar role under Commonwealth law. Unlike the PIPA, consent is defined in the Privacy Act and means 'express consent or implied consent'.[190] 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;
- gives consent voluntarily; and
- 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).[191]

2.3.62 The Guidelines also highlight new technologies which can collect information, in circumstances where it may be impossible or very difficult to obtain consent.

2.3.63 The ACCC has made important recommendations about amending the Privacy Act to strengthen consent requirements, including consideration of:

> Strengthening consent requirements to require that consents are freely given, specific, unambiguous and informed and that any settings for additional data collection must be preselected to 'off'. Consents should be required whenever personal information is collected, used or disclosed by an entity subject to the Privacy Act, unless the personal information is necessary to perform a contract to which a consumer is a party, required under law, or otherwise necessary in the public interest.[192]

2.3.64 This recommendation reflects the approach to consent under the GDPR,[193] where it includes 'any freely given, specific, informed and unambiguous indication of the data subject's wishes by

[189] OAIC, *Submission to Privacy Act Review* (n 26) 46 (recommendations 18 and 19).
[190] *Privacy Act 1988* (Cth) s 6(1).
[191] OAIC, *Australian Privacy Principles Guidelines* (n 149) ch B, [B.48]–[B.51].
[192] ACCC, *Digital Platforms Inquiry* (n 72) 24.
[193] See GDPR (n 29) arts 4(11), 7. Article 7 stipulates the 'conditions for consent'.

which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'. The ACCC's recommendation is to adopt the higher standard of consent provided for in the GDPR in order to bolster the level of protection provided in the Privacy Act.[194]

2.3.65 In its submission to the Privacy Act review, the OAIC generally agreed with strengthening the current consent requirements that apply to circumstances where there is a high risk of privacy concerns arising. This includes:

- requiring notices to be concise, transparent, intelligible, and written in clear and plain language;[195]
- requiring the use of standardised icons;[196] and
- requiring that notices should also include information on how an individual can withdraw their consent.[197]

2.3.66 However, the OAIC cautioned against relying on notice and consent requirements in routine privacy settings. Personal information is collected and shared across an increasingly complex range of devices, situations, and purposes. Applying strengthened consent requirements in a wholesale manner may impose unnecessary compliance burdens on custodians. Further, it also risks turning consent into a 'tick-box exercise which will detract the value of consent in higher-risk situations where it will actually be valuable'.[198] The OAIC therefore recommended that consent requirements be augmented with general fairness and reasonableness requirements on all personal information handling (discussed next).

2.3.67 Relying on consent to validate a custodian's information handling practices also raises concerns over the treatment of children and others with limited capacity to consent. PIPP 2 on disclosure recognises that disclosure of personal information to a parent may be suitable in some circumstances. However, PIPP 1 on *collection* does not make particular provision regarding who is being asked to consent to the collection of personal information. In comparison, the privacy principles in NSW include the possibility of collecting information from a person's guardian where the Individual concerned is under 16.[199]

2.3.68 In calling for the strengthening of consent requirements in its Digital Platforms report, the ACCC noted that users of digital platforms often include children who likely lack the capacity to truly understand how their personal information is collected, used, and disclosed. The Commission therefore recommended that children should only be able to consent through their guardian.[200]

2.3.69 In some circumstances, it may not be practicable to obtain a child's consent through their guardian, such as in many online settings or in relation to the information collected through use of devices which include an internet connection. Therefore, the Commission recommended that additional requirements to minimise collection of personal information from children who engage with digital platforms and ensure meaningful guardian consent should be addressed in an online privacy code of conduct for this context.[201]

[194] ACCC, *Digital Platforms Inquiry* (n 72) 465.
[195] OAIC, *Submission to Privacy Act Review* (n 26) 77 (recommendation 32).
[196] Ibid 75 (recommendation 33).
[197] Ibid 80 (recommendation 36).
[198] Ibid 69.
[199] *Privacy and Personal Information Protection Act 1988* (NSW) s 9.
[200] ACCC, *Digital Platforms Inquiry* (n 72) 468. The ACCC drew on article 8 of the GDPR and also the United States' *Children's Online Privacy Protection Act 1998*: 15 USC §§ 6501–6506 (1998).
[201] ACCC, *Digital Platforms Inquiry* (n 72) 468.

Fairness and reasonableness requirements

2.3.70 As has been discussed, under Tasmanian law, PIPP 1 requires the collection of personal information to be done by lawful means, whereas under Commonwealth law, APP 3 requires collection to be not only lawful, but also fair. However, this fairness requirement does not similarly extend to the *use* or *disclosure* of personal information.

2.3.71 In its submission to the Privacy Act review, the OAIC recommended that fairness and reasonableness requirements apply to collection, use, and disclosure of personal information. This requirement would apply even where the individual has consented to the particular form of information handling.

2.3.72 The OAIC also recommended that a non-exhaustive list of factors be set out in legislation for use in determining whether information handling is fair and reasonable in the circumstances. These would reflect requirements in other jurisdictions,[202] including:

- whether the purposes for collection, use, or disclosure will have unjustified adverse impacts on any individual;
- whether the purposes are reasonable, necessary, and proportionate;
- whether the actual collection, use, or disclosure will intrude into an individual's personal affairs; and
- whether the actual collection, use, or disclosure is within the reasonable expectation of the individual concerned.[203]

2.3.73 Further, the OAIC recommended that there should be full or partial prohibitions on certain types of information handling practices. This could include practices with a high risk of privacy intrusion, such as:

- practices aimed at children, including profiling, tracking, or behavioural monitoring, or direct advertising;
- inappropriate surveillance or monitoring of an individual through audio or video functionality of the individual's mobile phone or other personal devices;
- scraping of personal information from online platforms; and
- handling location information about individuals.

2.3.74 Various uses of artificial intelligence technology to make decisions about individuals could also be subject to additional requirements to ensure their use meets the fair and reasonableness standard (see discussion below on artificial intelligence, at [2.3.86]–[2.3.90]).

2.3.75 Incorporating a fair and reasonableness 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 regulate the above practices and other emerging privacy risk practices with an approach that aligns with those in other jurisdictions.

[202] This recommendation reflects article 5(1)(a) of the GDPR, which provides for the fairness principle alongside principles of lawfulness and transparency.
[203] OAIC, *Submission to Privacy Act Review* (n 26) 86–7.

Right to object

2.3.76 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.

2.3.77 Once an objection is raised, processing of the data must cease unless an exception applies. The applicability of the two exceptions depend on why the data was lawfully collected without the individual's consent in the first place, as set out below.

- If the collection was done in the public interest or was an exercise of lawful authority, the entity must stop processing the data unless it is being used in relation to legal claims or if there are compelling legitimate grounds for processing the information—grounds which outweigh the interests, rights and freedoms of the individual.
- If the collection was for scientific, historical research or statistical purposes, the entity must stop processing the data, unless the processing is necessary for performing a task that is carried out for public interest reasons.

2.3.78 The GDPR also expressly addresses the situation where information is processed for direct marketing purposes, and allows individuals to object at any time to such use of their personal data. Once notified, the entity must stop using the data in this way.

2.3.79 In its submission to the Privacy Act review, the OAIC recommended that the Act adopt a similar right to object. This complemented its recommendation to repeal APP 7 on direct marketing.[204]

2.3.80 If incorporated into the PIPA, a general right to object could apply to a range of situations, including any use of personal information for direct marketing by non-government bodies. It 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.

Right of erasure

2.3.81 Under the GDPR, the right to object complements the right to erasure, otherwise known as a 'right to be forgotten'. Article 17 of the GDPR provides for this 'right to be forgotten' in some circumstances. Where it 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.

2.3.82 The 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 above;
- the information was collected through use of an online service by a child, including where the parent or guardian consented; or

[204] Ibid 54–5 (recommendation 25).

- the information was collected, used or disclosed or otherwise handled in an unlawful way.

2.3.83 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.[205]

2.3.84 The ACCC's Digital Platforms Inquiry recommended that Australia adopt such 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.[206] The OAIC has similarly recommended that a right to erasure be adopted. It suggested that it would complement existing requirements to destroy or de-identify information that is no longer needed, and should extend to information that is no longer held by the custodian but is placed on social media networks. Any such right would also be subject to appropriate timeframes.[207]

2.3.85 If adopted in the PIPA, a right to erasure would be subject to exceptions where retention is necessary for archiving purposes or is otherwise required by law. It would also require personal information custodians to take reasonable steps to inform other custodians of any request for erasure. This would prevent proliferation of personal information across multiple custodians and would require custodians to consider whether it remains necessary to retain information.

Use of Artificial Intelligence ('AI')

2.3.86 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.[208] 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.

2.3.87 Article 22 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: it can only be used in automated processes where explicit consent has been given or it is authorised by legislation.
- *Non-sensitive* data: it 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.

2.3.88 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.

[205] See GDPR (n 29) art 89 in relation to the requirements for archiving purposes.
[206] ACCC, *Digital Platforms Inquiry* (n 72) 473.
[207] OAIC, *Submission to Privacy Act Review* (n 26) 52–4.
[208] See, eg, GDPR (n 29) art 4 (definition of 'profiling').

2.3.89 The Australian Human Rights Commission ('AHRC') has recognised the various 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 to governments using decision-making systems informed by artificial intelligence to make administrative decisions.[209] 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;[210]
- providing for mechanisms to independently review the merits of any decision made;[211]
- 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;[212] and
- requiring reasons or a technical explanation of the decision to be given before a decision can be considered lawful.[213]

2.3.90 In general, requiring transparency, monitoring, and accountability of AI may protect against inappropriate or unduly invasive use of personal information. Such regulations regarding government use of AI could be included in the PIPA or in separate but complementary legislation.

Questions:	
2.7	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?
2.8	Are there any other amendments to the PIPPs that you think should be made?
2.9	Should any of the other potential reforms be introduced, including: a. fairness and reasonableness requirements; b. a right to object; c. a right to be forgotten; d. specific restrictions on the use of artificial intelligence in automated administrative decision-making; or e. strengthened notice and consent requirements?

[209] AHRC, *Human Rights and Technology Final Report* (n 143) ch 5.
[210] Ibid 55 (recommendation 2).
[211] Ibid 68 (recommendation 8).
[212] Ibid 60 (recommendation 3).
[213] Ibid 62 (recommendation 5).

2.4 Complaints, monitoring, and enforcement

Complaints process

2.4.1 Under the Tasmanian PIPA, a person affected by a breach of the PIPPs can make a complaint to the Tasmanian Ombudsman[214] within six months from the date they first became aware of the alleged breach, unless the Ombudsman permits additional time.[215] Before the complainant approaches the Ombudsman, however, they must ensure that the PIPP applies to them, and the complainant must also try to resolve the matter with the relevant personal information custodian.[216] The requirement that the PIPP apply to the complainant generally requires that they are the person identified or identifiable in the information in question.

2.4.2 If these requirements have been met, the Ombudsman is then able to conduct a preliminary assessment of the complaint, including requesting further information from the complainant and the personal information custodian.[217] Following the preliminary investigation, the Ombudsman may decide to:

- resolve the complaint expeditiously (without conducting further investigations beyond the preliminary assessment);[218]
- *not* deal with the complaint if satisfied that the complaint is either: 1) frivolous, vexatious, lacking in substance or is not in good faith; 2) trivial; or 3) relates to a matter permitted or required under any law;[219] or
- refer the complaint to another person or body the Ombudsman considers appropriate to investigate or take other action, which must only be done after consultation with both the complainant and relevant person or body to whom the complaint is referred.[220]

2.4.3 If none of the above apply and the Ombudsman decides to deal with the complaint, the Ombudsman conducts a formal investigation using the process and powers set out in Division 3 of the *Ombudsman Act 1978* (Tas).[221] For example, the Ombudsman must give written notice of the investigation to the complainant and the public authority being investigated, and must allow anyone who might be subject to adverse comments in the report a chance to appear before the Ombudsman or otherwise make representations.[222] The Ombudsman has extensive powers, including entering the premises of public authorities,[223] and compelling people to provide information or give evidence.[224] An investigation by the Ombudsman must, however, be conducted in private.[225]

2.4.4 Once the investigation is completed and if the Ombudsman determines 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.[226] The opinion and any recommendations are provided to the Minister and tabled in both Houses of Parliament within five sitting days of receipt.

---

[214] PIPA (n 40) s 18.
[215] 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).
[216] Ibid s 18(1)–(2).
[217] Ibid s 19.
[218] Ibid s 19(1A).
[219] Ibid s 19(2).
[220] Ibid s 20.
[221] Ibid s 21.
[222] *Ombudsman Act 1978* (Tas) s 23A.
[223] Ibid s 25
[224] Ibid s 24
[225] Ibid s 23A(3).
[226] PIPA (n 40) s 22.

2.4.5 Table 2.1 (below) shows data from the Ombudsman's annual reports, listing the numbers of complaints received by agency.[227]

Table 2.1 Number of privacy complaints to Tasmanian Ombudsman 2018–22, by agency type (%)

Agency	**2018–19** **N (%)**	**2019–20** **N (%)**	**2020–21** **N (%)**	**2021–22** **N (%)**
State government departments	382 (52.5)	344 (53.5)	378 (53)	508 (56)
Local government	76 (10.5)	81 (12.7)	77 (13)	88 (10)
Public authorities and GBEs	119 (16.2)	66 (10.3)	69 (10)	93 (10)
Out of jurisdiction	150 (20.6)	131 (20.4)	170 (20)	188 (21)
Personal Information Protection	4 (<1)	14 (2.1)	17 (3)	11 (1)
Public Interest Disclosure	4 (<1)	6 (1)	4 (1)	19 (2)
Total	**735 (100)**	**642 (100)**	**715 (100)**	**907 (100)**

2.4.6 It should be noted that the Tasmanian Ombudsman cannot initiate own motion investigations—with no power to investigate a breach of the PIPPs or other general issues under the PIPA if there has been no complaint.[228] The Ombudsman can, however, initiate an own motion investigation into administrative action taken by public authorities and government contractors, including information handling practices.[229]

2.4.7 Further, the PIPA does not make provision for an individual to appeal or seek review if they are dissatisfied with the actions or recommendations of the Ombudsman.[230] This limit on the private rights of action where there has been a complaint made by an individual against a personal information custodian can be contrasted with the wider range of such rights under Commonwealth, NSW, and Victorian privacy legislation.[231] For more detailed discussion of review options in other jurisdictions, see the section below on private rights of action (at [2.4.14]).

[227] Ombudsman Tasmania, *Annual Report 2021–2022* (Report, 2022) <https://www.ombudsman.tas.gov.au/__data/assets/pdf_file/0007/683251/Final-signed-Ombudsman-Annual-Report-2021-2022.PDF> 12.
[228] 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).
[229] See *Ombudsman Act 1978* (Tas) s 12.
[230] 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.
[231] See, eg, *Privacy Act 1988* (Cth) s 96; *Privacy and Personal Information Protection Act 1988* (NSW) s 3; *Privacy and Data Protection Act 2014* (Vic) pt 3 div 8.5.

Remedies for breach of privacy

Compensation

2.4.8 The Tasmanian PIPA does not directly provide for compensation for a breach of privacy principles, in contrast to privacy legislation in NSW,[232] Victoria,[233] Queensland,[234] and in the Commonwealth jurisdiction. For example, in the latter, after an investigation under the Privacy Act, the OAIC can declare that 'the complainant is entitled to a specified amount by way of compensation for any loss or damage suffered by reason of the act or practice the subject of the complaint'.[235] This includes humiliation and injury to feelings.[236] The payable amount is enforceable as a debt due.[237]

2.4.9 In the period 2018–19, the OAIC reported 111 conciliated privacy complaints in which compensation was an agreed remedy, with nine complaints involving compensation of over $10,000.[238] Conciliated privacy complaints are where the OAIC helps parties resolve the complaint between themselves, rather than determining it for them.

Penalties and other enforcement actions

2.4.10 The Tasmanian PIPA does not provide for any penalties when a PIPP is breached. In contrast, the Commonwealth Privacy Act provides for a range of civil penalty measures associated with certain breaches under that Act, including for serious and repeated interferences with privacy.[239] These civil penalty provisions are enforceable by the OAIC seeking a court order that the contravener pay a pecuniary penalty.[240] There are some instances of breach of a privacy principle where the relevant provision does not carry a civil penalty, for example, there is no penalty for a one-off minor breach. Further, even if a civil penalty order is available, the OAIC will not decide in every case that such an order is the appropriate enforcement option.[241]

2.4.11 The OAIC is also able to enforce provisions of the Privacy Act by seeking an injunction before, during, or after an investigation or exercise of other regulatory powers,[242] or by accepting an enforceable undertaking.[243] Enforceable undertakings are used where there has already been, or appears to have been, a privacy interference. The entity itself or the OAIC may raise this option as the appropriate enforcement measure. An enforceable undertaking seeks to have the entity voluntarily agree to modify their acts, remedy any damage the breach used, and commit to future measures to

---

[232] *Privacy and Personal Protection Act 1988* (NSW) s 53(7)(c) provides for internal review by the agency in question. This review may in turn be reviewed by the NSW Civil and Administrative Tribunal (NCAT): *Privacy and Personal Protection Act 1988* (NSW) s 55. NCAT is able to make an order of up to $40,000 by way of compensation for any loss or damage suffered because of the conduct.

[233] *Privacy and Data Protection Act 2014* (Vic) s 77(1)(a) allows the Victorian Civil and Administrative Tribunal, after reference by the Information Commissioner where a complaint about a breach of privacy has not been able to be conciliated, to make an order not exceeding $100,000 'by way of compensation for any loss or damage suffered by the complainant, including injury to the complainant's feelings or humiliation suffered by the complainant, by reason of the act or practice the subject of the complaint'.

[234] *Information Privacy Act 2009* (Qld) s 178(a)(v) allows the Queensland Civil and Administrative Tribunal, after a complaint has been referred by the Information Commissioner after mediation was not achieved, to award up to $100,000 'to compensate the complainant for loss or damage suffered by the complainant because of the act or practice complained of, including for any injury to the complainant's feelings or humiliation suffered by the complainant'.

[235] *Privacy Act 1988* (Cth) s 52(1)(b)(iii).

[236] Ibid s 52(1AB).

[237] Ibid s 60.

[238] OAIC, *Annual Report 2018–19* (Report, September 2019) 161.

[239] *Privacy Act 1988* (Cth) s 13G. The remaining civil penalty provisions relate to the Credit Reporting protections in Part IIIA.

[240] See *Privacy Act 1988* (Cth) s 80U.

[241] OAIC, *Guide to Privacy Regulatory Action* (Guidance Document, June 2020) ch 6 [6.17].

[242] Ibid s 80W.

[243] Ibid s 80V.

comply with privacy obligations. The terms of an enforceable undertaking are negotiated between the entity and the OAIC staff, and if accepted by the Australian Information Commissioner, are ultimately enforceable in court.[244]

2.4.12 In submissions to the review of the Privacy Act, the OAIC has asked for additional enforcement powers. These include extending the ability to seek civil penalties to all privacy interferences, as well as allowing for the OAIC to make orders to mitigate foreseeable risks or delete personal information when it determines that there has been a privacy interference.[245]

2.4.13 In Victoria, there is an enforcement option not found in either the PIPA nor the Privacy Act. The Victorian Information Commissioner has the option of serving a compliance notice for repeat, serious or flagrant contraventions of privacy principles.[246] Failure to comply with the notice is a criminal offence.[247] There is a right to seek review of a decision to serve a compliance notice.[248]

Private rights of action

2.4.14 Under the Tasmanian PIPA, an individual seeking redress for breach of a PIPP is limited to seeking review from the personal information custodian in question and then making a complaint to the Ombudsman. Other jurisdictions in Australia provide alternative ways for an individual to initiate review of a potential breach.

- Commonwealth: individuals can seek to have OAIC decisions reviewed by the Administrative Appeals Tribunal[249] or federal courts.[250] The Tribunal conducts merits review—reviewing both the factual and legal basis for the OAIC's decision, and can set aside, vary, or affirm the decision. The court conducts judicial review—meaning it only determines whether or not the decision was *lawful* (for example, whether the OAIC 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 OAIC for re-consideration and decision but cannot re-make the decision itself.
- Queensland: complaints can be referred to the Queensland Civil and Administrative Tribunal for merits review if mediation is not reasonably likely or has not been successful.[251] Like conciliation, mediation is where the Queensland Information Commissioner works with the parties to help them agree on options to resolve the complaint.
- Victoria: like in Queensland, the Victorian Information Commissioner can refer complaints to the Victorian Civil and Administrative Tribunal for merits review where conciliation is not appropriate or has failed. The Minister can also directly refer complaints to the Tribunal.[252]
- NSW: a person who is aggrieved by a breach of a privacy obligation can seek internal review (review within the agency who allegedly breached the obligation). The NSW Privacy Commissioner is informed of the review and may make submissions or carry out the review at the request of the agency. Decisions from the internal review can further be reviewed by the NSW Civil and Administrative Tribunal.

[244] OAIC, *Guide to Privacy Regulatory Action* (n 241) ch 3.
[245] OAIC, *Submission to Privacy Act Review* (n 26) 129.
[246] *Privacy and Data Protection Act 2014* (Vic) s 78.
[247] Ibid s 82.
[248] Ibid s 83.
[249] *Privacy Act 1988* (Cth) s 96.
[250] *Administrative Decisions (Judicial Review) Act 1977* (Cth) s 5; OAIC, *Guide to Privacy Regulatory Action* (n 241) ch 4 [4.24].
[251] *Information Privacy Act 2009* (Qld) pt IV.
[252] *Privacy and Data Protection Act 2014* (Vic) s 73.

2.4.15 Under Commonwealth law, the Privacy Act also allows individuals to seek an injunction in court. Injunctions can restrain an entity from contravening any provision in the Act or can require them to do a certain thing.[253]

2.4.16 Other than injunctions, however, there is no direct right of action to seek compensation or other orders from the court. The Privacy Act review raised the possibility of enabling individuals to go to court to seek damages for privacy interferences under the Act.[254] The ACCC made similar recommendations concerning damages for financial and non-financial harm suffered as a result of the interference.[255] In its submission to the Privacy Act review, the OAIC agreed and made further suggestions on how such a right might be framed.[256]

Other regulatory action

Privacy Impact Assessments

2.4.17 Under Commonwealth law, the OAIC can request that government agencies undertake a privacy impact assessment.[257] This is a written assessment that identifies how an activity or function will impact on the privacy of individuals and that sets out recommendations for managing, minimising, or eliminating that impact.[258] Failure to comply with a direction to produce a privacy impact assessment is reported to the Minister responsible for the agency. The Tasmanian PIPA does not contain equivalent provisions for such assessments.

Privacy Codes

2.4.18 Another possible gap under the Tasmanian PIPA is 'privacy codes'. These codes of practice augment privacy principles 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. Commonwealth, NSW, and Victorian privacy legislation provide for mechanisms to develop and approve privacy codes.

2.4.19 Under the Commonwealth Privacy Act, codes of practice about information privacy may be developed by the OAIC directly,[259] or by entities either on their own initiative or upon request by the Australian Information Commissioner.[260] The codes set out how one or more APPs are to be applied or complied with, and may also impose additional requirements.[261] The Commissioner registers approved codes on the Codes Register.[262] As of 1 October 2021, there were three registered privacy codes.[263] One example is the *Privacy (Australian Government Agencies – Governance) APP Code 2017*, discussed above at [2.3.28]–[2.3.29].

2.4.20 If the Tasmanian PIPA was amended to provide for the development of such codes, or to provide for similar rules to be made in delegated legislation, it could enhance the transparency of privacy risks at early stages in the development of new Tasmanian government projects.

---

[253] *Privacy Act 1988* (Cth) s 80W; *Regulatory Powers (Standard Provisions) Act 2014* (Cth) s 121.
[254] OAIC, *Submission to Privacy Act Review* (n 26) 69.
[255] ACCC, *Digital Platforms Inquiry* (n 72) 472–3.
[256] OAIC, *Submission to Privacy Act Review* (n 26) 129.
[257] *Privacy Act 1988* (Cth) s 33D.
[258] 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>.
[259] *Privacy Act 1988* (Cth) s 26G.
[260] Ibid s 26E.
[261] Ibid s 26C.
[262] Ibid ss 26F–26H.
[263] *Privacy (Credit Reporting) Code 2014*; *Privacy (Australian Government Agencies – Governance) APP Code 2017*; Privacy (Market and Social Research) Code 2021: see OAIC, *Privacy Codes Register* (2020) <https://www.oaic.gov.au/privacy/privacy-registers/privacy-codes-register/>

Mandatory data breach notification

2.4.21 Under Tasmanian law, if a personal information custodian deals with information in a way which breaches the PIPPs, it is *not* obliged under the PIPA to inform the Ombudsman or the individual concerned. In contrast, under Commonwealth law, a mandatory data breach notification scheme has operated since February 2018.[264] The scheme requires all entities subject to the Privacy Act to investigate and report 'eligible data breaches' to the OAIC and to the individuals in the information. This is intended to allow affected individuals to take steps to minimise any harm, encourage entities to better comply with privacy obligations, and promote transparency of information handling practices.[265]

2.4.22 'Eligible data breaches' arise when the following three conditions are satisfied:[266]

- there has been unauthorised access to or disclosure of personal information, or alternatively, information is *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 the list of factors in section 26WG;[267] and
- no remedial action that would prevent the likely risk of serious harm has been taken.

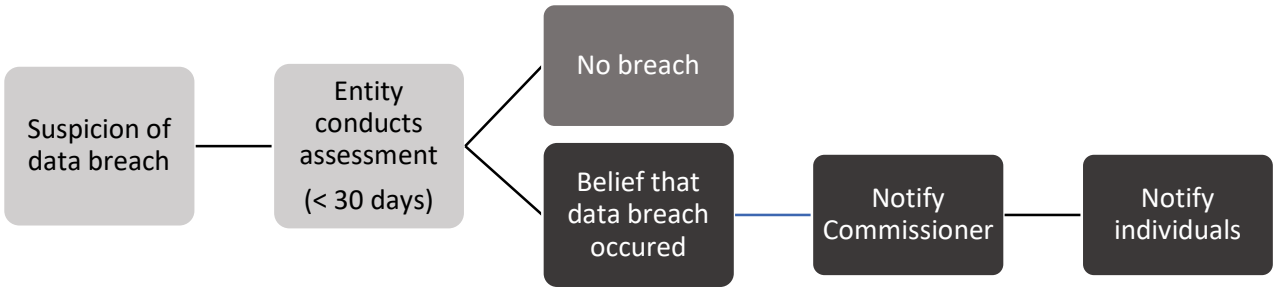
2.4.23 Whether the entity must notify the Australian Information Commissioner and the individuals concerned depends on whether the entity *suspects* a data breach has occurred, or whether it *believes* that such a breach has occurred (belief requires a higher degree of certainty than suspicion).

2.4.24 Once 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. It must take all reasonable steps to complete this assessment within 30 days.[268] The Privacy Act does not set out how to conduct an assessment—entities develop their own processes.[269]

2.4.25 If during the assessment process or after it is complete, the entity becomes aware of reasonable grounds to *believe* there has been an eligible data breach, it must inform the Australian Information Commissioner as soon as practicable.[270] After notifying the Commissioner, the entity must take reasonable steps to inform the individuals affected, either by communicating directly with them or through general publicity where direct communication is not practicable.[271]

[264] *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth).
[265] Attorney-General's Department, *Privacy Amendment (Notifiable Data Breaches) Bill 2016 Regulation Impact Statement* (Regulation Impact Statement, 11 January 2017) 15.
[266] *Privacy Act 1988* (Cth) ss 26WE–26WG.
[267] This includes how sensitive the information is and who has obtained it.
[268] *Privacy Act 1988* (Cth) s 26WH.
[269] OAIC, *Data Breach Preparation and Response: A Guide to Managing Data Breaches in accordance with the Privacy Act 1988 (Cth)* (Guidance Document, July 2019) 47 ('*Data Breach Preparation and Response*').
[270] *Privacy Act 1988* (Cth) s 26WK.
[271] Ibid 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* (n 269) 48.

Figure 2.1 Mandatory eligible data breach notification scheme (simplified)



2.4.26 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.[272] From January to July 2021, there were 446 notifications including 85 from private health service providers and 34 from the Australian government.[273] Causes of breaches were identified as follows: 65% involved malicious or criminal attack; 30% involved human error; and 5% were due to a system fault.[274]

2.4.27 On the whole, the obligations under the Commonwealth scheme are less onerous (in terms of timeframes) than those under the GDPR. Generally, the GDPR requires notification of personal data breaches[275] without undue delay and, where feasible, within 72 hours of the entity having become aware of it.[276] The individuals affected must be informed whenever the breach is likely to result in a high risk to their privacy rights.[277]

2.4.28 The current review of the Commonwealth Privacy Act includes consideration of the effectiveness and operation of mandatory data breach notifications. This includes issues such as 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.[278] The NSW government is considering whether to adopt a similar mandatory reporting scheme.[279] These issues also relevant to consider in the Tasmanian context.

[272] OAIC, *Notifiable Data Breaches Scheme 12-month Insights Report* (Report, 13 May 2019) 8.
[273] OAIC, *Notifiable Data Breaches Report: January to June 2021* (Report, August 2021) 7.
[274] Ibid 14.
[275] 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 (n 29) art 4.
[276] Ibid art 33.
[277] Ibid art 34.
[278] OAIC, *Submission to Privacy Act Review* (n 26) 138–45.
[279] A discussion paper was released in July 2019 and submissions closed on 23 August 2019: NSW Government, *Mandatory Breach Notification* (Web Page, 2019) <https://www.justice.nsw.gov.au/justicepolicy/Pages/lpclrd/lpclrd_consultation/mandatory-data-breach-notification.aspx>

Questions:	
2.10	How effective is the current complaints process in enforcing obligations under the PIPA?
2.11	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?
2.12	What other remedies should be available to individuals affected by a breach of the PIPA?
2.13	Are there other forms of enforcement action that should be introduced?
2.14	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?
2.15	Should a form of data breach notification requirement be introduced? If so, what models of mandatory reporting schemes should be considered?

Part 3

3 Other legislation impacting the privacy of government-held information

3.1 Introduction

3.1.1 This section of the Issues Paper continues to focus on government-held information, but looks beyond the *Personal Information Protection Act 2004* (Tas) ('PIPA') at other legislative provisions that impact the privacy of such information. It discusses situations where legislation may override the privacy protections in the PIPA ([3.2]); where legislation may impose secrecy obligations that can serve as privacy protections ([3.3]); and 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 ([3.4]).

3.2 Legislation which may override the PIPA

3.2.1 The privacy protections offered by the PIPA can be overridden by any inconsistent provisions in other legislation.[280] Therefore, 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. 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.

3.2.2 For example, the *Right to Information Act 2009* (Tas) provides a legally enforceable right to be provided with information possessed by a public authority or a Minister.[281] This is subject to various exemptions that allow information to be withheld. For example, information can be withheld if disclosure would include a third party's personal information and is contrary to the public interest.[282] While the public interest could nevertheless weigh in favour of disclosure, the third party should first be consulted and may apply for review of any decision to disclose their information.

3.2.3 As for whether there is inconsistency with the PIPPs, it is unclear whether the reference to 'public interest' would limit disclosure to the various circumstances where disclosure is permitted under the PIPPs. In other words, it is unclear whether disclosure that would breach the PIPPs would be deemed *against* the public interest under the *Right to Information Act 2009* (Tas).

3.2.4 On the other hand, a clear and direct example of inconsistency is found in legislation relating to Stolen Generation investigations. The law 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.[283]

---

[280] PIPA (n 40) s 4.
[281] *Right to Information Act 2009* (Tas) s 7. The Tasmanian Ombudsman has determined that the PIPA does not prevent release of personal information under the *Right to Information Act 2009* (Tas): *Clive Stott and Hydro Tasmania* [2021] Ombudsman Tasmania, Decision 1702–115 [69].
[282] *Right to Information Act 2009* (Tas) s 36. See s 33 about the public interest test. See also ss 37, 39 for other exemptions subject to a public interest test, including disclosure of information relating to the business interests of a third party and information communicated in confidence.
[283] *Stolen Generations of Aboriginal Children Act 2006* (Tas) s 16(2).

3.3 Legislation that restricts the sharing of government-held information

3.3.1 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, to prevent them from using or disclosing information in an unauthorised way. Unauthorised disclosure may be subject to penalties.[284]

3.3.2 For example, there are secrecy obligations on:

- law enforcement officers in the context of financial reporting;[285]
- individuals administrating the first home owner grant scheme;[286]
- individuals dealing with occupational licensing;[287]
- officers dealing with the registration of those authorised to work with vulnerable people;[288]
- individuals involved in the governance of the Australian Crime Commission,[289] Corporate Affairs,[290] and Consumer Affairs;[291] and
- individuals involved in processing workers' rehabilitation and compensation claims.[292]

3.3.3 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 found under the PIPA, there are exceptions for when information can nevertheless be disclosed.[293] 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;[294]
- in relation to carrying out functions under or in administration of the legislation in question;[295]
- considered necessary or appropriate in the public interest generally;[296]
- related to legal proceedings;[297]

---

[284] See, eg, *First Home Owner Grant Act 2000* (Tas) s 40(3).
[285] *Financial Transaction Reports Act 1993* (Tas) s 10.
[286] *First Home Owner Grant Act 2000* (Tas) s 40.
[287] *Occupational Licensing Act 2005* (Tas) s 51.
[288] *Registration to Work with Vulnerable People Act 2013* (Tas) s 54.
[289] *Australian Crime Commission Act 2004* (Tas) s 44.
[290] *Commissioner for Corporate Affairs Act 1980* (Tas) s 6E.
[291] *Consumer Affairs Act 1988* (Tas) s 22.
[292] *Workers Rehabilitation and Compensation Act 1988* (Tas) s 158.
[293] 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.
[294] *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.
[295] *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.
[296] *Gaming Control Act 1993* (Tas) s 157*; Vehicle and Traffic (Driver Licensing and Vehicle Registration) Regulations 2010* (Tas) s 125.
[297] *Threatened Species Protection Act 1995* (Tas) s 59.

- related to research or statistical analysis purposes;[298] or
- only to specified agencies or officers, who may, but may not, be subject to restrictions on the handling of the information in question.[299]

3.3.4 In some cases, these restrictions may be considered proportionate 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.

3.4 Legislation that facilitates the sharing of information within and between government agencies

3.4.1 Legislative provisions may provide for the gathering of personal information *without* specifically providing for limitations on its use or sharing. This can jeopardise information privacy. An example is legislation that facilitates information sharing within and between government-agencies.

Tasmania

3.4.2 The sharing of 'basic personal information'[300] with public authorities represents a potential gap in protection under the PIPA. As discussed above at [2.2.53]–[2.2.55], 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. There may therefore be considerable scope for Tasmanian government agencies to share certain information without being restricted by obligations under the PIPA or by other privacy considerations.

3.4.3 Information is vital to good government. It is an asset that is essential for developing informed policy, and data exchange across agencies provides for better government-wide statistical capability. Therefore, the Tasmanian Government has adopted the Administrative Data Exchange Protocol for Tasmania ('ADEPT'), to 'promote and manage cross-Agency information exchange in ways that are open, transparent and secure'.[301]

3.4.4 The ADEPT is intended to be read in conjunction with the PIPA and 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. 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 the ADEPT recognises, much of 'data considered essential for population-based research and policy decisions contains personal and often sensitive information'.[302]

3.4.5 As part of this principle, agencies must follow ADEPT procedures to ensure the 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.

---

[298] *Asbestos-Related Diseases (Occupational Exposure) Compensation Act 2011* (Tas) s 184.
[299] *First Home Owner Grant Regulations 2010* (Cth) s 6.
[300] The name, residential address, postal address, date of birth, and gender of an individual: PIPA (n 40) s 3 (definition of 'basic information').
[301] The Department of Premier and Cabinet, 'ADEPT Principles', *Tasmanian Government* (Web Page) <http://www.dpac.tas.gov.au/divisions/digital_strategy_and_services/policies/digital_data_privacy/adept>.
[302] Ibid.

3.4.6 However, generally speaking, there are limited *additional* privacy safeguards included in the ADEPT principles and procedures, and no independent means to enforce the ADEPT requirements.

Other jurisdictions

3.4.7 In contrast, other jurisdictions have taken or are planning to develop measures to provide for the sharing of government-held information within and between agencies in a way that is more consistent, and which seeks to preserve privacy protections.

3.4.8 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.[303] Agencies must comply with NSW privacy legislation[304] and other privacy safeguards, including using contractual measures to restrict the use of information shared with non-government agencies and reporting potential privacy contraventions.[305]

3.4.9 At the Commonwealth level, the Data Availability and Transparency Bill 2020[306] has been introduced following recommendations of the Productivity Commission in their Data Availability and Use inquiry.[307] The Productivity Commission commented that:

> [l]ack of trust by both data custodians and users in existing data access processes and protections and numerous hurdles to sharing and releasing data are choking the use and value of Australia's data.

3.4.10 The proposed legislation is intended to provide authority for government agencies to share information between themselves and various other organisations, defined as 'accredited users'. It will permit data sharing only for the purposes of delivering government services, informing government policy and programs, and research and development. Agencies must seek the consent of any individuals before sharing personal information unless it is unreasonable or impracticable to do so. Any sharing must comply with data sharing principles that 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.

3.4.11 However, even with these protections concerns have been raised in consultation on the proposed Bill regarding whether the potential privacy impacts are justified.[308]

3.4.12 Another proposal at the Commonwealth level is the Identity-matching Services Bill 2019, discussed above (see [2.2.3]). This seeks to authorise the exchange of identity information between

---

[303] *Data Sharing (Government Sector) Act 2015* (NSW) s 6.
[304] *Privacy and Personal Information Protection Act 1998* (NSW); *Health Records and Information Privacy Act 2002* (NSW).
[305] See *Data Sharing (Government Sector) Act 2015* (NSW) pt 3.
[306] Data Availability and Transparency Bill 2020 (Cth).
[307] Productivity Commission, *Data Availability and Use Final Report* (Report, May 2017) <https://www.pc.gov.au/inquiries/completed/data-access/report>.
[308] See Senate Standing Committee for the Scrutiny of Bills, Parliament of Australia, *Scrutiny Digest* (Digest No 5 of 2021, 17 March 2021); Senate Finance and Public Administration Legislation Committee, Parliament of Australia, *Data Availability and Transparency Bill 2020 [Provisions] and Data Availability and Transparency (Consequential Amendments) Bill 2020 [Provisions]* (Report, 29 April 2021); Parliamentary Joint Committee on Human Rights, Parliament of Australia, *Report 4 of 2021* (Report, 31 March 2021).

Commonwealth, state, and territory governments for use with identity-matching services, including facial recognition services.[309]

3.4.13 More generally, Commonwealth, state, and territory Governments have also signed an intergovernmental agreement 'to share data across jurisdictions as a default position,[310] where it can be done securely, safely, lawfully and ethically'.[311] Consistent with the Data Availability and Transparency Bill 2020, information will be shared according to data sharing principles.[312] Governments also committed to identifying and removing restrictions that unnecessarily impede lawful data sharing, and to ensuring that security and privacy obligations continue to apply to any shared information.

3.4.14 These initiatives in other jurisdictional contexts 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 the Tasmanian context, it must be ensured that privacy safeguards apply whenever legislation authorises personal information to be shared within and between government agencies and contractors.

Questions:	
3.1	Should legislation providing for the application of minimum privacy safeguards be introduced to apply to all information sharing within and between government bodies?
3.2	If such legislation should be introduced, how should the safeguards be enforced?

[309] Identity–matching Services Bill 2019 (Cth).
[310] In other words, share data unless some law or other rule precludes such sharing.
[311] *Intergovernmental Agreement on Data Sharing between Commonwealth and State and Territory governments*, signed 9 July 2021 <https://federation.gov.au/about/agreements/intergovernmental-agreement-data-sharing>.
[312] Office of the National Data Commissioner, *Best Practice Guide to Applying Data Sharing Principles* (Guidance Document, 15 March 2019).

Part 4

4 Other protections of privacy

4.1 Introduction

4.1.1 In addition to the *Personal Information Protection Act 2004* (Tas) ('PIPA'), there are other existing privacy protections under Tasmanian law that apply in various contexts and are contained in either legislation or in judicial statements in case law. While this Issues Paper has so far focused largely on information privacy, these other protections may also deal with other types of privacy, such as bodily privacy, privacy of communications, or territorial privacy.

4.1.2 Legislation includes protection against various forms of harm to privacy interests. However, these are generally limited to activities or circumstances in which specific interferences with privacy might occur. These include governmental or workplace surveillance, stalking, harassment, and image-based abuse (previously called 'revenge pornography').

4.1.3 Tasmanian courts have had few opportunities to consider privacy. Even when an opportunity has arisen, it has rarely been considered as a stand-alone right or cause of action requiring a remedy. Rather, it has largely only been considered when relevant legislation refers to or incorporates privacy in particular contexts.

4.1.4 More broadly, in some limited circumstances of particularly egregious privacy interferences, Australian courts have at least *recognised* the need to protect individual privacy. However, there is currently no recognised civil remedy at common law that covers interferences with privacy in a comprehensive, rather than context-dependent, manner. Instead, the courts have mostly resorted to equitable remedies to vindicate individual privacy, such as by finding that someone was subject to obligations of confidentiality and awarding damages in compensation for breach.

4.1.5 Recently the High Court has recognised, under constitutional law, the protection of privacy as a legitimate purpose justifying what would otherwise be an impermissible burden on the implied freedom of political communication.[313] This too, however, has not amounted to a concrete remedy specifically for breaches of privacy. It represents only a nascent development, giving rise to proposals to develop a new comprehensive civil remedy for interference with privacy.

4.2 Legislative protections

Health information

4.2.1 The *Health Complaints Act 1995* (Tas) provides for the making, investigation, conciliation, and reference of complaints against public and private health services. Grounds for complaint include that the provider failed to respect the privacy or dignity of someone using the service, or that the provider acted unreasonably in denying access to a user's records or disclosing information in relation to a user.[314]

4.2.2 For the purposes of this Act, 'health services'[315] is broadly defined to mean a service provided to a person for, or purportedly for, the benefit of human health. This covers:

- medical, dental, pharmaceutical, or mental health services;
- aged care or disability care;

[313] *Clubb v Edwards*; *Preston v Avery* (2019) 267 CLR 171.
[314] *Health Complaints Act 1995* (Tas) s 23.
[315] This can be compared to the definition of 'health service' in the PIPA, see above at [2.2.37].

- 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.

4.2.3 This broad definition covers both[316] services provided at certain places, such as hospitals or nursing homes, and services provided by various listed health professionals.

4.2.4 The *Health Complaints Act 1995* (Tas) also provides for the establishment and review of the Health Rights Charter.[317] The *Tasmanian Charter of Health Rights and Responsibilities* was developed under this provision and sets out privacy rights for health service consumers. Compliance with the Charter is one of the grounds for complaint under the Act,[318] and must be taken into account when assessing whether a health service's actions were reasonable.[319]

4.2.5 Some rights listed in the Charter relate to information to ensure active participation in health care and confidentiality, privacy and security of information. This includes 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 his/her health is 'kept securely and cannot be easily accessed by unauthorised persons'.[320]

4.2.6 Complaints must be assessed by the Health Commissioner within 45 days, and either: referred to an appropriate body such as the Ombudsman or a relevant professional registration board; referred for conciliation; investigated; or dismissed. The Health Commissioner also has the power to investigate matters referred to them by the Health Minister or on their own initiative.

4.2.7 The Act facilities the making and investigating of complaints in various ways. It overrides legislation that hinders the disclosure of information, if such hindrance would prevent or restrict the making of a complaint or the conduct of investigations.[321] It also confers extensive investigation powers on the Health Commissioner, including the power to compel provision of documents, examine witnesses, apply for warrants, and enter any premises occupied or used by a health service or a health service provider. 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.[322] However, if the recording, disclosure, or use of statistical or other information could not reasonably be expected to lead to the identification of any person, then it is not limited under the Act.[323]

4.2.8 While the *Health Complaints Act 1995* (Tas) deals with information privacy, other legislation may touch 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,

---

[316] *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: at sch 1 pt 2.
[317] *Health Complaints Act 1995* (Tas) ss 17, 20. The Charter must reflect principles such as effective patient participation in health decisions, patients taking an active role in their health care, preservation of the confidentiality of a patient's health information, and access to a patient's own health records.
[318] Ibid s 23(1)(k).
[319] Ibid s 75.
[320] *Tasmanian Charter of Health Rights and Responsibilities* arts 1, 3.
[321] *Health Complaints Act 1995* (Tas) s 62B.
[322] Ibid 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.
[323] Ibid s 65(5).

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.[324]

Surveillance

4.2.9 Two main pieces of legislation in Tasmania provide protections against 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)**

4.2.10 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.[325] 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.[326]

4.2.11 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 journalists can record interviews and how people may use drones.

4.2.12 The Act also sets out consequences of breaching the prohibitions, specifying offences relating to the general prohibition on recording private conversations.[327] If law enforcement personnel obtain evidence unlawfully under the Act, this limits the circumstances in which the evidence can be used in court.[328] 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.[329]

4.2.13 While the general rule is a prohibition on the use of listening devices, there are exceptions.[330] They include:

- warrants issued under the Act for law enforcement activities;[331]
- activities authorised under other legislation, including Commonwealth legislation;[332]
- unintentional hearing through use of a listening device;
- recording interviews between a police officer and a person suspected of having committed a statutory offence;
- consent; and
- where evidence or information needs to be obtained through a listening device in connection with various serious offences or threats.[333]

[324] *Forensic Procedures Act 2000* (Tas) ss 34K(1)(b), 35(a).
[325] *Listening Devices Act 1991* (Tas) s 5(1).
[326] Ibid s 3(1).
[327] With penalties up to maximum imprisonment of two years and/or 40 penalty units (or 500 penalty units for a corporation): ibid s 12.
[328] Ibid pt III.
[329] Ibid s 21.
[330] Ibid ss 5(2)-(7).
[331] Ibid pt IV.
[332] *Telecommunications (Interception) Act 1979* (Cth); *Police Powers (Surveillance Devices) Act 2006* (Tas).
[333] 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).

4.2.14 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.[334] 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.[335]

4.2.15 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.

4.2.16 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.[336] The Supreme Court has reiterated that this factor must be considered.[337] 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.

4.2.17 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.[338] Senior officers may also authorise use of a surveillance device in emergency circumstances.[339] Amendments introduced in 2018 also permit the use of a personal camera by on-duty police officers to record private conversations.[340] To this extent, this Act permits law enforcement officers to interfere with privacy.

4.2.18 However, under this Act, the power to undertake surveillance under warrants is subject to monitoring, review, and inspection.[341] 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).[342]

***Police Offences Act 1935* (Tas)**

4.2.19 The *Police Offences Act 1935* (Tas) provides that it is an offence to observe or visually record another person in breach of privacy.[343] This is another general prohibition on surveillance—in this case, visual observation rather than listening to private conversations. As with offences provided under the *Listening Devices Act 1991 (Tas*), the offence is not limited to any specific type of device and would cover the use of drones.

4.2.20 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) is 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.

[334] Ibid s 5(4); see also s 5(7).
[335] Ibid s 6(2).
[336] Ibid s 17(2).
[337] *Kirkland v Tippett* [2000] TASSC 94 (19 July 2000).
[338] *Police Powers (Surveillance Devices) Act 2006* (Tas) s 9.
[339] Ibid pt 3.
[340] *Surveillance Legislation Amendments (Personal Police Cameras) Act 2018* (Tas).
[341] *Police Powers (Surveillance Devices) Act 2006* (Tas) pt 5.
[342] Ibid ss 32–3.
[343] *Police Offences Act 1935* (Tas) s 13A(1).

4.2.21 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).[344] 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.

4.2.22 Closely related to this offence, the *Police Offences Act 1935* (Tas) also makes it an offence to:

- possess a prohibited visual recording;[345]
- publish or distribute such a recording;[346] 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).[347]

4.2.23 Regarding this range of offences of observing and recording in breach of privacy, there are three categories of people who are excluded from criminal responsibility, provided that they meet the onus of proving that they fall within one of three categories. They are as follows:[348]

- a law enforcement officer acting reasonably in the course of performing his or her duties;
- a person acting reasonably in the course of his or her duties in relation to someone who is in lawful custody (for example, officers in prisons); and
- a person acting in the course of his or her occupation or employment and where his or her conduct is reasonable in that context.

4.2.24 In essence, people who fall within these three categories are lawfully permitted to interfere with individuals' privacy through observation or visual recording.

Drones

4.2.25 The Commonwealth House of Representatives Standing Committee on Social Policy and Legal Affairs has commented that '[r]emotely piloted aircraft have the potential to pose a serious threat to Australians' privacy. They can intrude on a person's or a business's private activities either intentionally, as in the case of deliberate surveillance, or inadvertently.'[349]

4.2.26 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.[350] However, there are no legislative limitations that explicitly and specifically relate to privacy.

4.2.27 Tasmania does not have regulations that limit how RPAs or UVAs (drones) can interfere with privacy. However, as discussed earlier in this part, drones are encompassed within the general criminal prohibitions on the use of listening devices and on observing or visually recording people. Drones may also be subject to limitations in the law of civil wrongs, specifically nuisance and

[344] *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).
[345] *Police Offences Act 1935* (Tas) s 13C.
[346] Ibid s 13B.
[347] Ibid s 13A(2).
[348] Ibid s 13D.
[349] Commonwealth House of Representatives Standing Committee on Social Policy and Legal Affairs, *Report: Eyes in Sky; Inquiry into Drones and the Regulation of Air Safety and Privacy* (Report, 14 July 2014) 33 [4.1].
[350] See, eg, *Civil Aviation Safety Regulations 1998* (Cth) ss 101.025, 101.055.

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.

Stalking and harassment

4.2.28 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). These behaviours may cause humiliation, psychological distress, or intimidation in the same way as egregious interferences with privacy.[351]

4.2.29 In Tasmania, various legislation prohibits harassment and similar behaviour. Where harassment, 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 harassment, stalking, and bullying.

4.2.30 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.[352] Stalking or bullying means pursuing a course of conduct involving one or more behaviours listed in the provision. 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.

4.2.31 Although this crime covers a reasonably wide range of behaviours that could amount 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.
- Even if prosecution is commenced and there is a finding of guilt, it will not necessarily result in any remedies for the victim in the same way as there may be 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.[353]
- 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 very difficult for a prosecutor to prove this 'mental element' of knowledge.[354]

[351] 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).
[352] *Criminal Code* (Tas) s 192.
[353] Ibid s 192(2).
[354] In this context, 'knowledge' refers to what the defendant actually knew, or what they ought to have known. See also ibid s 13.

4.2.32 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 door to door trading,[355] family relationships (harassment can lead to a Police Family Violence Order being imposed),[356] solicitors' conduct when engaging in court processes (particularly regarding how clients are advised and witnesses are treated),[357] and public transport.[358]

4.2.33 Further, the *Sex Discrimination Act 1994* (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.[359] 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.

Unauthorised sharing of intimate images

4.2.34 The Commonwealth Parliament has legislated to protect individuals from online harassment and unauthorised (online) sharing of intimate images. The underlying rationale is to address instances of image-based abuse and other egregious, largely online, interferences with privacy.

4.2.35 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.[360] 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, blackmail, shaming, or demeaning them.

4.2.36 The 2018 Act also amended the *Enhancing Online Safety Act 2015* (Cth) to create civil penalty offences for posting intimate images on social media without a person's consent. 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.

4.2.37 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 cyber-bullying and image-based abuse.[361] This Act is intended to operate concurrently with state and territory laws.[362]

4.2.38 Some jurisdictions also have specific voyeurism offences which operate concurrently with the Commonwealth laws. For example, the *Crimes Amendment (Sexual Offences) Act 2008* (NSW)

[355] *Door to Door Trading Act 1986* (Tas) s 12.
[356] *Family Violence Act 2004* (Tas) ss 14(3)(d)–(f).
[357] *Legal Profession (Solicitors Conduct) Rules 2000* (Tas) regs 26(1)(c), (2)(c), (8)(a)(ii).
[358] *Passenger Transport Regulations 2000* (Tas) regs 20(2)(b)–(d).
[359] *Sex Discrimination Act 1994* (Tas) s 17(1).
[360] *Criminal Code Act 1995* (Cth) vol 2 sch, s 474.17A.
[361] Supplementary Explanatory Memorandum, Online Safety Bill 2021 (Cth) 1.
[362] *Online Safety Act 2021* (Cth) s 234.

introduced specific offences concerning voyeurism and filming a person engaged in a private act. Similar offences have also been introduced in Queensland, the ACT, Victoria, and South Australia.

4.2.39 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*. This led to nearly all states and territories passing laws that introduced offences concerning the distribution of images without consent.[363] Notably, Tasmania remains the current exception where such crimes have *not* been introduced.

4.2.40 In NSW, the *Crimes Amendment (Intimate Images) Act 2017* inserted four new offences into the *Crimes Act 1900* (NSW), including recording,[364] distributing,[365] threatening to record,[366] and threatening to distribute an intimate image without consent.[367] The maximum penalties are three years' imprisonment and/or a $11,000 fine. The amendment legislation also provided new definitions for these offences, including for 'intimate image', 'private parts', and 'engaged in a private act'.[368]

4.2.41 In Tasmania, the Civil Digital Communications Bill 2017 (Tas) was introduced in 2017 and intended to 'address the issues pertaining to persons who send or deliver electronic communications, letters or other articles for the purpose of causing distress or anxiety'.[369] The Bill proposed the creation of an offence of harassment where the course of conduct involves disclosing private sexual photographs and films with intent to cause distress.[370] The Bill also proposed the prohibition of electronic stalking (including monitoring a person's online activities),[371] putting people in fear of violence,[372] and obtaining private sexual material for use.[373] The Bill also proposed remedies in the form of injunctions and take down orders, on application to the Magistrates' Court.[374]

4.2.42 Therefore, the Bill would have provided remedies for individuals who are the victims of egregious, harmful, and intentional online interferences with privacy, including image-based abuse. However, while the Bill passed its first reading in the House of Assembly on 18 October 2017,[375] it did not progress further and has not been reintroduced in the current Parliament.

Other Tasmanian legislation referring to privacy

4.2.43 Legislation that governs broader matters not related to individual privacy may nevertheless have provisions that include references to privacy. The below list is a representative pool of such legislative provisions. They indicate where the Tasmanian Parliament has been prepared to raise privacy as a factor to be considered, largely because the power, activity, or situation in question gives rise to use of private information or potential intrusion on privacy. However, it should be noted that the provisions may also provide for privacy protections to be reduced or waived, particularly where a contrary public interest is in question.

[363] In NSW, these offences were introduced in the *Crimes Amendment (Intimate Images) Act 2017* (NSW) and in Queensland through the *Criminal Code (Non-consensual Sharing of Intimate Images) Amendment Act 2017* (Qld).
[364] *Crimes Act 1900* (NSW) s 91P.
[365] Ibid s 91Q.
[366] Ibid s 91R(1).
[367] Ibid s 91R(2).
[368] Ibid s 91N.
[369] Civil Digital Communication Bill 2017 (Tas).
[370] Ibid cls 5–8.
[371] Ibid cl 9.
[372] Ibid cl 11.
[373] Ibid cl 12.
[374] Ibid cls 10, 13.
[375] Parliament of Tasmania, 'Civil Digital Communications Bill 2017' (Web Page, 2021) <https://www.parliament.tas.gov.au/Bills/Bills2017/62_of_2017.html>.

- The *Children, Young Persons and Their Families Act 1997* (Tas): mandates that a child be treated with respect, including that the child is a valued member of society, entitled to be treated in a manner respecting his or her dignity and privacy.[376]
- The *Disability Services Act 2011* (Tas): mandates that persons with a disability should have their privacy and dignity respected.[377] Failure of a health provider to do so is grounds for complaint under the *Health Complaints Act 1995* (Tas).[378]
- The *Residential Tenancy Act 1997* (Tas): all non-social housing residential tenancy arrangements must include window coverings for privacy.[379]
- The *Access to Neighbouring Land Act 1992* (Tas): if a person needs to access neighbouring land to carry out work (for example, to repair drains), and the court grants an order permitting such access, the order may be subject to conditions to avoid or minimise loss of privacy.[380]

4.2.44 These references to privacy do not provide for concrete or comprehensive privacy protection, nor do they provide a foundation for a principle of individual privacy. However, they represent an acknowledgment by the Tasmanian Parliament that, at least in particular circumstances, individual privacy may be affected and may be required to be taken into account in how a power is exercised or an activity is undertaken.

4.3 Judicial references to privacy and the development of general law protections

4.3.1 There have been very few cases concerning interference with privacy in Australia overall, and even fewer in Tasmania in particular. While Tasmanian courts have had opportunities to comment on the value of privacy, such cases have not centred on privacy interferences. Rather, comments have been made in limited circumstances where legislation refers to privacy (for example, as a factor to be considered in an assessment) or where a party invokes international instruments protecting privacy.

4.3.2 In some cases of egregious interferences, 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. However, they have not recognised a standalone privacy right or civil remedy that comprehensively covers privacy interferences.

The value of privacy before the Tasmanian courts

Admissibility of evidence

4.3.3 One example where this arises is when determining whether or not evidence that was improperly or illegally obtained should be admitted into court. Courts have a discretion to refuse such evidence if the desirability of admitting the evidence outweighs the *undesirability* of admitting evidence that was obtained improperly or illegally.[381] One matter to be considered is whether the manner of obtaining evidence was contrary or inconsistent with a right recognised in the *International Covenant on Civil and Political Rights* ('ICCPR').[382]

[376] *Children, Young People and Their Families Act 1997* (Tas) s 10D(1).
[377] *Health Complaints Act 1995* (Tas) s 5(1)(j).
[378] Ibid s 123(1)(f).
[379] *Residential Tenancy Act 1997* (Tas) s 36N(1).
[380] *Access to Neighbouring Land Act 1992* (Tas) s 6(2)(b).
[381] *Evidence Act 2001* (Tas) s 138.
[382] Ibid s 138(3)(f).

4.3.4 In discussing this rule, the Supreme Court has acknowledged that it encompasses the right in article 17 of the ICCPR to not be subjected to arbitrary or unlawful interference with privacy.[383] In some cases, the Court has found that the impugned evidence was inadmissible because the way in which it was obtained involved an interference with the accused's privacy and violated article 17.[384]

4.3.5 The case of '*Hibble'* involved the admissibility of DNA evidence where the accused was a minor. The Tasmanian Supreme Court found that the evidence was inadmissible as it had been improperly obtained not only in contravention of article 17, but also because it involved an arbitrary interference with the child's privacy in contravention of the *Convention on the Rights of the Child*.[385]

4.3.6 More recently, the case of '*Wykes'* involved the evidence of a self-described 'paedophile hunter' who pretended to be a young boy when communicating with the accused online, and who then set up an in-person meeting with the intention of recording footage and posting it to YouTube for public denouncement.[386] In a decision of the Supreme Court, Chief Justice Blow recognised 'the dangers inherent in the sort of vigilante exposure practised by the witness, including: dangers to the people denounced through social media, their families, their houses and their property; danger to vigilantes who act in such a way; the danger of driving people to suicide; and the danger of compromising police investigations'.[387]

Administration of justice

4.3.7 The Supreme Court has also acknowledged that privacy interests will be set aside in the context of the administration of justice—relevant to court proceedings. In this context, the principle of public accountability and exposure takes precedence, and the requirement of open justice must be upheld.[388] Open justice demands that court proceedings be open to public for scrutiny. It is a fundamental right and freedom of the public in a democratic society that values fair trials.

4.3.8 This stands, despite recognition that it is common for sensitive, extremely personal, or confidential issues to be litigated and disclosed in court. The principle is reflected in the specific context of witness cross-examination—questions are not disallowable merely because they require the witness to discuss a subject that they may consider private.[389] Similarly, while concealing the identity of a particular party might be in the interests of that individual and their privacy, perhaps even their safety, it can only be departed from in exceptional circumstances.[390]

Balancing exercise

4.3.9 In a 1996 decision, the Supreme Court of Tasmania acknowledged—in the context of a property planning scheme dispute—that the issue of privacy was a matter of degree, and that not all interferences would be taken in law to have unreasonably diminished an individual's privacy.[391]

4.3.10 More recently, the Court has recognised that legislation referring to privacy interests is underpinned by a parliamentary intention to strike a balance between personal privacy and countervailing public interests. In '*Melick*,' the balance was between the privacy of mail versus

[383] Ibid s 138(3)(f). See also *R v Brown* [2014] TASSC 18; *R v Pettit* [2015] TASSC 14; *Tasmania v Wykes* [2019] TASSC 18.
[384] *Hibble v B* [2012] TASSC 59; *R v Brown* [2014] TASSC 18; *R v Pettit* [2015] TASSC 14; *Tasmania v Wykes* [2019] TASSC 18. 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.
[385] *Hibble v B* [2012] TASSC 59 [76]. The provisions violated in the Convention were arts 16.1 and 16.2.
[386] *Tasmania v Wykes* [2019] TASSC 18 [1]–[7].
[387] Ibid [38].
[388] *Sierra 4 v Moles* [1994] TASSC 38 [61]–[67].
[389] *Evidence Act 2001* (Tas) s 41(3)(b).
[390] *Sierra 4 v Moles* [1994] TASSC 38.
[391] *Carnevale v Baker* [1996] TASSC 9 [20].

interests in effective crime detection.[392] A parcel containing illicit drugs was x-rayed and opened during processing. The contents were disclosed to police. Relevant legislative provisions contained a general prohibition on the opening of parcels, but contained exceptions authorising customs officers to open articles reasonably believed to consist of, or contain, certain drugs or other chemical compounds.

4.3.11 Whether it is this context, or in the context of evidence law or the administration of justice, Tasmanian courts have treated privacy as an important value to be considered in appropriate circumstances. However, it has been treated it as a *qualified* value—it may only be legally protected if interferences are unreasonable, and it must be set aside when countervailing public interests carry greater weight in the circumstances.

Tort law (civil wrongs)

4.3.12 No appellate court in Australia and no Tasmanian court has recognised a tort of interference with privacy, whether it includes information privacy, physical privacy, or both. Nor has any such court granted remedies in tort law for interferences with privacy.

4.3.13 In '*Lenah Game Meats*',[393] the High Court of Australia considered the possible legal claims that might prevent the broadcasting of footage taken from inside a corporate-owned abattoir without permission. These legal claims included whether an action in tort was available. Ultimately, there was no actionable interference with privacy. However, this turned on the fact that it was a *corporation*, not a human person, bringing the claim. The High Court found that any right of privacy could only be sought by a natural person. Corporations have legal 'personality', but are not natural persons. They could not, in principle, be entitled to any right in privacy or any remedy arising out of a breach of privacy.

4.3.14 Despite the outcome, each of the judgments arguably left the door open for a standalone action for interference with individual privacy, however it is framed, to be recognised by Australian courts when the appropriate facts arise.[394] In each individual judgment, their Honours 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.

4.3.15 The High Court in *Lenah Game Meats* also suggested that privacy protection from Australian common law was not necessarily excluded following a 1937 case that is often cited for its rejection of a right to privacy, that of '*Victoria Park Racing'*.[395] More recently, the High Court has again confirmed that Australian courts are not precluded from recognising a tort of interference with privacy and granting tortious remedies, including compensation for harm suffered.[396]

4.3.16 Since *Lenah Game Meats*, there has been inconsistency among lower courts in Australian jurisdictions towards granting remedies for interferences with privacy. Some have done so, including by granting damages under a tort of invasion of privacy.[397] Others have refused to recognise any such

[392] *Tasmania v Melick* [2019] TASSC 19 [13], [20](d), citing *Australian Postal Corporation Act 1989* (Cth) pt VII(B) s 90T.
[393] *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* (2001) 208 CLR 199 ('*Lenah Game Meats*').
[394] See Gligorijevic, 'Reaffirming *ABC v Lenah Game Meats*' (n 7).
[395] *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479; see eg, *Lenah Game Meats* (n 393) [185]–[189].
[396] *Smethurst v Commissioner of the Australian Federal Police* (2020) 94 ALJR 502, [48], [86], [129].
[397] *Grosse v Purvis* [2003] QDC 151; *Doe v Australian Broadcasting Corporation* [2007] VCC 281.

action, whether as a tort or otherwise, even where the plaintiff is an individual rather than a corporation.[398]

4.3.17 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 (discussed next).[399]

4.3.18 The Supreme Court of Tasmania has not had an opportunity, since the High Court decision of *Lenah Game Meats*, to adjudicate a claim seeking tortious or other remedies for interference with privacy.

Equity

4.3.19 As just mentioned, two Australian appellate courts have considered the availability of remedies for interferences with privacy.

4.3.20 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.[400]

4.3.21 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*).[401]

Recognition of privacy in constitutional settings

4.3.22 Under the *Commonwealth Constitution*, there is an implied right of freedom of political communication. If legislation burdens this right, one step of the test of whether it is a *justifiable* burden is whether its legislative objective is 'legitimate'—whether it is compatible with maintaining the system of representative government as established by the *Constitution*. If yes, the means used must still be 'appropriate and adapted' to serving the end. This latter question involves, in part, assessing whether the importance of the purpose is proportionate to the extent of the restriction.[402]

4.3.23 The High Court recognised the protection of privacy as a legitimate objective in a case involving legislation that limited the freedom of individuals to protest outside abortion clinics.[403] The case incorporated an appeal from the Magistrates' Court of Tasmania,[404] and the Tasmanian Solicitor-General submitted that the prohibition on protests 'can readily be seen to serve the purpose of

[398] *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].
[399] *Giller v Procopets [No 2]* (2008) 24 VR 1; *Wilson v Ferguson* [2015] WASC 15.
[400] *Wilson v Ferguson* [2015] WASC 15.
[401] See Gligorijevic, 'Reaffirming *ABC v Lenah Game Meats*' (n 7); JD Heydon, MJ Leeming and PG Turner, *Meagher, Gummow and Lehane's Equity: Doctrines and Remedies* (LexisNexis Butterworths, 5th ed, 2015) 882–3; PG Turner, 'Privacy Remedies Viewed through an Equitable Lens' in Jason NE Varuhas and NA Moreham (eds), *Remedies for Breach of Privacy* (Hart Publishing, 2018) 265.
[402] *Comcare v Banerji* (2019) 372 ALR 42, 54 [29].
[403] *Clubb v Edwards; Preston v Avery* (2019) 267 CLR 171.
[404] *Police v Preston and Stallard* [2016] (27 July 2016) TASMC 14.

protecting the safety, wellbeing, privacy and dignity of persons accessing premises where terminations are provided.'[405] The High Court of Australia accepted these submissions.

4.3.24 In the judgment, the majority of the Court reasoned that a justified and proportionate limitation on the implied freedom of political communication could be found in a fundamental right to privacy, cognisable in Australian common law. It was through reference to this right to privacy that the legislation justified protecting healthcare autonomy and security by creating a protected space where protests against certain healthcare decisions were prohibited. The legislative purpose of protecting an individual's right to privacy, informed as it was by the value of individual dignity, was therefore compatible with the maintenance of the constitutionally prescribed system of representative and responsible government.[406]

4.3.25 Separate from the implied freedom of political communication, the High Court has also recognised the possible importance of privacy in the grant of an injunction against an officer of the Commonwealth under section 75(v) of the *Constitution*. This was decided in the context of a legal challenge brought against the federal police for searching a journalist's private residence and seizing information from their phone.[407]

4.3.26 It is noted that three Australian states have statutes codifying human rights or fundamental rights. These contain a qualified statutory right to privacy.[408] However, as the rights are contained in ordinary state or territory legislation, they can be set aside, limited, or otherwise interfered with by other legislation.

4.4 A civil cause of action for interference with privacy

4.4.1 As this Issues Paper has noted, there is currently no civil cause of action (and therefore no remedy) in Australia that covers interferences with privacy in a comprehensive manner. Instead, there are various sources of law and remedies for those causes of action, including under the PIPA, that cover various types of privacy in various contexts. Some legal scholars in Australia have engaged with the prospect of a civil remedy for interference with privacy in Australia with a view to, among other things, addressing gaps where protection is lacking—particularly in relation to physical privacy of the person.[409]

4.4.2 The existing provisions and remedies may invoke privacy, relate to privacy, or happen to protect or vindicate privacy. They may cover some common, or increasingly more common, situations involving interference with privacy. However, it may be that the fragmented landscape of existing provisions and remedies does not cover all situations, regardless of context, in which there may be an interference with or reasonable expectation of privacy, especially physical privacy.

[405] *Clubb v Edwards; Preston v Avery* (2019) 267 CLR 171 [120].
[406] Ibid [49]–[51].
[407] *Smethurst v Commissioner of the Australian Federal Police* (2020) 272 CLR 177, [73], [120], [246]. A privacy tort was not pleaded in this case and the Court therefore, explicitly, declined to consider it on the facts: see at [46], [48], [90], [129], [244]. For an analysis of privacy as a common law constitutional right in the United Kingdom, see K Hughes, 'A Common Law Constitutional Right to Privacy — Waiting for Godot?' in M Elliott and K Hughes (eds), *Common Law Constitutional Rights* (Hart Publishing, 2019).
[408] *Charter of Human Rights and Responsibilities Act 2006* (Vic) s 13; *Human Rights Act 2004* (ACT) s 12; *Human Rights Act 2019* (Qld) s 25.
[409] 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*' (n 7).

4.4.3 The piecemeal nature of existing protections is demonstrated by the following examples outlining some of the situations that could involve interferences with privacy, which are not necessarily covered by existing legislation or general law:

- misuse of private information by non-governmental actors, including the media, journalists, advertising corporations, and data processing entities;[410]
- 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;[411]
- use of private information for the purposes of blackmail;[412]
- aggressive media reportage activities, including 'door-stepping' and 'grief journalism';[413]
- 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;[414]
- 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);[415]

[410] 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 413 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.

[411] 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*' (n 7); and Turner (n 401) 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.

[412] 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).

[413] For a recent 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.

[414] See Jelena Gligorijevic, 'Children's Privacy: The Role of Parental Control and Consent' (2019) 19(2) *Human Rights Law Review* 201.

[415] 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.

- 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;[416]
- '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;[417]
- 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);[418]
- use of RPAs and UAVs (drones) in a way that is intended to have or in fact has the effect of intruding upon an individual's physical privacy;[419] and
- general intrusions upon seclusion, whether or not they involve audio-visual recording.[420]

4.4.4 The discussion in this section raises a general issue as to whether Tasmania needs a comprehensive civil statutory cause of action (and remedy) for privacy interference. As courts in Australia and other jurisdictions, such as New Zealand, have been reluctant to recognise such a cause of action,[421] if it were to be introduced into legislation, it could operate in addition to the existing web of legal protections. If such a cause of action were to exist, the scope and limits of such a comprehensive protection also require consideration.

[416] 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.
[417] 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).
[418] See, eg, *Murray v Big Pictures Ltd* [2008] 3 WLR 1360; *Weller v Associated Newspapers Ltd* [2016] 1 WLR 1541.
[419] As noted above, there is no privacy-specific regulation on the use of drones in Australia.
[420] See, eg, *C v Holland* [2012] 3 NZLR 672 (High Court of New Zealand). See also NA 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.
[421] Eg *Peters v Attorney-General* [2021] 3 NZLR 191; *Hyndman v Walker* (2021) 12 NRNZ 503.

Questions:	
4.1	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?
4.2	Should there be stronger legislative protection, including through the introduction of new statutes in Tasmania, against governmental (particularly police) surveillance in general?
4.3	Should there be stronger legislative protection, including through the introduction of new statutes in Tasmania, against workplace surveillance in particular?
4.4	Should there be specific protection against interference with physical privacy through the use of drones (RPAs and UAVs)?
4.5	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?
4.6	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?
4.7	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?
4.8	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?
4.9	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?

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 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 include: 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

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). 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 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

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

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

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,[422] as well as the Information Privacy Principles Instruction, which is issued by Premier and Cabinet.[423] 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.[424]

Separately, the *Surveillance Devices Act 2016* (SA) regulates the use of surveillance devices.

Northern Territory

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.

The ACT is the other 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

[422] 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.
[423] 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.
[424] See Health and Community Services Complaints Commissioner, 'HCSCC Charter of Rights', available at https://www.hcscc.sa.gov.au/hcscc-charter-of-rights/.

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.[425]

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)).

[425] 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 Technologies* (Report No 77, February 2020)	Recommended the replacement of existing regulation on the use of surveillance devices by all persons.

Year	Jurisdiction	Title	Summarised recommendation
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.