Australian Government

Attorney-General's Department

Collecting, using and disclosing personal information for an integrity purpose:

November 2019

Guidance on Part VIID of the *Crimes Act 1914* (Cth)

Part VIID—Collecting, using and disclosing personal information that may be relevant for integrity purposes

86B Simplified outline of this Part

This Part authorises collection, use and disclosure of personal information for preventing, detecting, investigating or dealing with:

> *(a) serious misconduct by persons working for Commonwealth bodies; or*
>
> *(b) fraud affecting Commonwealth bodies; or*
>
> *(c) offences against Chapter 7 of the Criminal Code (which is about the proper administration of Government).*

The authorisation is relevant to laws (such as privacy laws) that limit the collection, use and disclosure of personal information unless authorised by law.

86C Target entity may collect sensitive information for integrity purpose

A target entity may collect for an integrity purpose sensitive information that:

> (a) if the target entity is a Privacy Act agency—is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or
>
> (b) if the target entity is a wholly-owned Commonwealth company—is reasonably necessary for one or more of the entity's functions or activities.

Note: Subclause 3.3 of Australian Privacy Principle 3 limits the circumstances in which an APP entity may collect sensitive information. This section lets a target entity collect sensitive information for an integrity purpose in circumstances corresponding to those in which it may collect other personal information (see subclauses 3.1 and 3.2 of that Principle).

86D Target entity may use personal information for integrity purpose

A target entity may use personal information for an integrity purpose relating to the entity.

86E Disclosure of personal information to target entity for integrity purpose

(1) This section applies if a law of the Commonwealth or of a State or Territory:

> (a) Limits disclosure of some or all personal information by a person, body or authority (however described); and
>
> (b) Exempts from the limitation a disclosure authorised by a law of the Commonwealth.

Note: Australian Privacy Principle 6 is an example of such a law of the Commonwealth. The Principle prohibits an APP entity from disclosing personal information for a purpose other than the one for which the entity collected the information, unless the disclosure is authorised under an Australian law or certain other exceptions apply.

(2) For the purposes of the exemption, the person, body or authority may disclose to a target entity for an integrity purpose personal information that the person, body or authority reasonably believes is related to one or more of the target entity's functions or activities.

Limit on subsection (2) for disclosures by target entity

(3) Subsection (2) applies to a disclosure by a target entity other than the Australian Federal Police only if it is made for the target entity by a person who is authorised to make disclosures for integrity purposes by:

(a) The accountable authority (within the meaning of the Public Governance, Performance and Accountability Act 2013) of the entity, if it is a Commonwealth entity; or

(b) The entity or its principal executive (within the meaning of the Privacy Act 1988), if it is a Privacy Act agency other than a Commonwealth entity; or

(c) A director of the entity, if it is a wholly-owned Commonwealth company.

86F This Part does not limit other laws

To avoid doubt, this Part does not impliedly limit other laws (whether written or unwritten) that authorise collection, use or disclosure of personal information.

86G Guidelines on the operation of this Part

(1) The Secretary of the Department may publish guidelines approved by the Information Commissioner on the operation of this Part.

(2) Guidelines under subsection (1) are not a legislative instrument.

Contents

Introduction

In August 2018, Parliament passed laws to better support Commonwealth agencies to collect, use and disclose personal information to prevent, detect, investigate or deal with fraud affecting the Commonwealth and other integrity purposes. The amendments were intended to address barriers caused, or perceived to be caused, by privacy laws. Importantly, these changes were intended to have broad application and be used for more proactive and preventative counter-fraud purposes.

The *Crimes Legislation Amendments (Powers, Offences and Other Measures) Act 2018* (Cth), which commenced on 25 August 2018, inserted a new Part VIID into the *Crimes Act 1914* (Cth) (Crimes Act). Part VIID authorises the collection, use and disclosure of personal information for preventing, detecting, investigating or dealing with:

- serious misconduct by persons working for Commonwealth bodies
- fraud affecting Commonwealth bodies, or
- offences against Chapter 7 of the *Criminal Code Act 1995* (Cth) (Criminal Code) (which is about the proper administration of Government).

The authorisation is relevant to laws (such as privacy laws) that limit the collection, use and disclosure of personal information unless authorised by law.

Under the *Public Governance, Performance and Accountability Act 2013* (Cth) (PGPA Act) and the Commonwealth Fraud Control Framework, Commonwealth entities are responsible for their own fraud and corruption control arrangements. This includes having appropriate controls and mechanisms in place to prevent and detect fraud and corruption. In the majority of cases, it is the agency itself (rather than a law enforcement agency) that will be responsible for investigating suspected incidents of fraud or corruption.

To effectively prevent, detect, investigate and deal with fraud and corruption, agencies should have timely access to relevant information from within their own agency and also from relevant external sources. The collection, use and disclosure of personal information by Commonwealth entities is regulated by various laws, including the *Privacy Act 1988* (Cth) (Privacy Act), state and territory privacy laws, and other secrecy and confidentiality provisions in agency or program specific legislation. Part VIID provides an authorisation for the purpose of privacy laws and some secrecy provisions to enable agencies to collect, use and disclose personal information to counter fraud and corruption.

This guidance outlines key terms and concepts associated with Part VIID and provides some case study examples of how Part VIID might be applied in practice.[1] Agencies may wish to consider seeking legal advice on the application of Part VIID to their specific circumstances.

[1] This guidance is made in accordance with section 86G of the Crimes Act, and has been developed in consultation with the Office of the Australian Information Commissioner (OAIC).

Definitions (A-Z)

Australian Privacy Principles

The Australian Privacy Principles (APPs) are the cornerstone of the privacy protection framework in the *Privacy Act 1988* (Cth). They apply to any organisation or agency covered by the Privacy Act. There are 13 APPs, which govern standards, rights and obligations around:

- the collection, use and disclosure of personal information
- an organisation or agency's governance and accountability
- integrity and correction or personal information
- the right of individuals to access their personal information.

Accountable Authority

Each Commonwealth entity has an accountable authority, which is generally the head or governing body of the entity.[2]

- If the Commonwealth entity is a Department of State or a Parliamentary Department, then the accountable authority of the entity is the Secretary of the Department.
- If the Commonwealth entity is a listed entity under the PGPA Act, then the accountable authority of the entity is the person or group of persons prescribed by an Act or the rules to be the accountable authority of the entity.
- If the Commonwealth entity is a body corporate, then the accountable authority of the entity is the governing body of the entity, unless otherwise prescribed by an Act or the rules.

Commonwealth Entity

A Commonwealth entity is a either a Department of State or a Parliamentary Department, listed entity, or body corporate that is established by a law of the Commonwealth. Further information about different types of Commonwealth entities can be found in the PGPA Act.[3]

Fraud

Fraud includes dishonestly obtaining a benefit, or causing a loss, by deception or other means. This may include (but is not limited to) activities such as theft, accounting fraud, providing false or misleading information to the Commonwealth, cartel conduct, and misuse of Commonwealth assets. The benefit or loss can be intangible, such as the loss of information. Further information is available in the Commonwealth Fraud Control Framework. It is not necessary to prove criminal intent for the purposes of Part VIID.

[2] See *Public Governance, Performance and Accountability Act 2013*, s 12.

[3] See PGPA Act, s 10. Part VIID of the Crimes Act differentiates between Target Entity, Privacy Act agency, Commonwealth entity and wholly-owned Commonwealth company in order to capture the broad variety of entities which could be considered to be Commonwealth agencies.

Integrity Purpose

Integrity purpose means the purpose of preventing, detecting, investigating or dealing with any of the following:

- misconduct of a serious nature by an official, person employed by or acting on behalf of a Commonwealth entity, a Privacy Act agency, or a wholly-owned Commonwealth company
- conduct that may induce or be intended to induce serious misconduct
- fraud that has or may have a substantial adverse effect on the Commonwealth or a target entity
- Chapter 7 Criminal Code offences (relating to the proper administration of government, such as theft and other property offences, fraudulent conduct, false or misleading statements, unwarranted demands, bribery and forgery).[4]

Misconduct

Misconduct includes fraud, negligence, default, breach of trust, breach of duty, breach of discipline or any other misconduct in the course of duty (consistent with the definition in the Privacy Act). The term misconduct is intended to cover behaviour that could be considered to be corruption.

Personal Information

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

- whether the information or opinion is true or not, and
- whether the information or opinion is recorded in a material form or not.

Common examples are a person's name, signature, address, telephone number, medical records, bank account details, and commentary or an opinion about the person.

Privacy Act Agency

Privacy Act agencies are government related agencies, individuals or bodies set out in the definition of agency in the Privacy Act.

Reasonably Necessary

The OAIC's non-binding *guidance on Australian Privacy Principle 3* indicates that **reasonably necessary** is an objective test that involves considering whether a reasonable person who is properly informed would agree that the action is necessary. It is the responsibility of the relevant entity to be able to justify that the particular collection, use or disclosure of personal information is reasonably necessary. Further information is available on the OAIC *website.*

Reasonable Belief

The OAIC's non-binding *guidance on key concepts in the Privacy Act* indicates that **reasonable belief** is taken to mean that an entity must have a reasonable basis for its belief, and not merely a genuine or subjective belief. A person must actually and honestly believe that there are real and substantial grounds for taking an action. It is the responsibility of an entity to be able to justify its reasonable belief.

[4] Crimes Act s 3(1).

Sensitive Information

Sensitive information refers to a specific subset of personal information which is particularly sensitive, and is therefore given a higher level of protection under the Privacy Act. Sensitive information includes information about a person's health, their religion, politics, racial or ethnic origin, and sexual orientation.

Substantial Adverse Effect

Subsection 3(1) of the Crimes Act defines substantial adverse effect as an effect that is adverse and not insubstantial, insignificant or trivial. In determining whether or not a case meets the threshold for substantial adverse effect, agencies should consider factors such as potential financial loss, duration of the fraud, the nature of the dishonest activity and non-financial loss or damage, including breaches of security and trust. Agencies should also consider the possibility that an incident that initially appears trivial or isolated could, upon further investigation, indicate a more sophisticated fraud, including fraud targeting multiple government programs.

Target Entity

A target entity is a Privacy Act agency or a wholly-owned Commonwealth company. This is a key term used in Part VIID, which captures the broad variety of entities that could be considered to be Commonwealth agencies or entities.

Trivial fraud or misconduct

Part VIID does not permit disclosure of personal information for trivial fraud or misconduct (as the definition of integrity purpose requires the fraud or misconduct to be 'serious'). Trivial fraud is any fraud that does not have a substantial adverse effect. Examples of trivial fraud or misconduct could be a one off incident of claiming extra time worked on a timesheet, or taking a low cost item of stationary from a workplace. These examples can still constitute misconduct, but should be dealt with through managerial response. Whether something is trivial or serious fraud or misconduct will depend upon the context. It is up to each target entity to determine its thresholds for trivial behaviour.

Wholly-owned Commonwealth company

A wholly-owned Commonwealth company is a Commonwealth company which has no shares beneficially owned by a person other than the Commonwealth. Further information is available in the PGPA Act.

Part VIID of the Crimes Act – guidance on key provisions

The *Crimes Legislation Amendment (Powers, Offences and Other Measures) Act 2018* amended the Crimes Act by adding new definitions to subsection 3(1), and inserting a new Part VIID.

Part VIID deals with the collection and use of personal information by, and the disclosure of personal information to, a target entity where that personal information may be relevant for integrity purposes.

- Section 86C allows a target entity to collect *sensitive* information for an integrity purpose, if the collection is reasonably necessary for, or directly related to, one or more of its functions or activities.
- Section 86D allows a target entity to use *personal* information for an integrity purpose relating to the entity.
- Section 86E authorises other Commonwealth, state and territory government and private sector entities to disclose *personal* information to a target entity for an integrity purpose.

As detailed in the definition section above, a *target entity* is a Privacy Act agency or a wholly-owned Commonwealth company.

An *integrity purpose* is also detailed in the definition section above. Integrity purposes include preventing, detecting, investigating or dealing with fraud or serious misconduct affecting the Commonwealth. Integrity purposes are not limited to criminal investigations and can involve administrative and civil action. If the integrity purpose is dealing with fraud other than a Chapter 7 Criminal Code offence, the fraud must have a 'substantial adverse effect' (that is, more than an insubstantial, insignificant or trivial effect) on the Commonwealth or target entity.

Part VIID came into effect on 25 August 2018, and may be relied upon to collect, use and disclose personal information for an integrity purpose from that date onwards. Information collected before this date may also be used and disclosed for an integrity purpose in accordance with Part VIID.

Collection of sensitive and personal information for an integrity purpose

Section 86C authorises target entities to collect *sensitive* information for an integrity purpose. The collection of *personal* information by target entities for an integrity purpose will generally be permitted by the Privacy Act in accordance with APP 3. However, the Privacy Act imposes stricter controls on the collection of sensitive information, which includes information about a person's health, religion, politics, racial or ethnic origin and sexual orientation. As sensitive information may be relevant to certain integrity purposes – for example, fraudulent claims of illness or injury – section 86C authorises the collection of sensitive information for an integrity purpose in appropriate circumstances corresponding to those in which an entity may collect other personal information.

The target entity will need to be able to demonstrate that the collection of sensitive information for an integrity purpose is reasonably necessary for one or more of the entity's functions or activities. This will depend upon the circumstances in each case, having regard to the nature of the entity's functions as well as the specific integrity purpose for which the information is to be collected. For example, it may be appropriate for an entity to collect information regarding a person's health to investigate fraudulent claims of illness or injury, but this would not require the agency to collect information about the person's religion or politics.

Use of personal information for an integrity purpose

Section 86D authorises target entities to use *personal* information for an integrity purpose relating to the entity. This section is intended to clarify, for the avoidance of doubt that personal information (including *sensitive* information) lawfully collected or disclosed to the target entity may be used by that entity for an integrity purpose.

A target entity 'uses' information where it handles or undertakes an activity with the information, within the entity's effective control. Examples include:

- the entity accessing and reading the personal information
- the entity searching records for the personal information
- the entity making a decision based on the personal information
- the entity passing the personal information from one part of the entity to another.

In limited circumstances, providing personal information to a contractor to perform services on behalf of the target entity may be a use, rather than a disclosure. This occurs where the entity does not release the subsequent handling of personal information from its effective control.

The personal information may have been collected by the agency in accordance with its own legal framework or under section 86C, it may have been disclosed to that target entity under section 86E, or otherwise legally obtained. Subject to other legislation, personal information can be used for a different integrity purpose to that which it was collected or disclosed, provided it meets the requirements under section 86D.

Disclosure of personal information for an integrity purpose

Section 86E authorises any person, body or authority to disclose personal information to a target entity for an integrity purpose in certain circumstances, if the person, body or authority disclosing the information reasonably believes that the personal information is related to one or more of the target entity's functions or activities.

Lawful authority

Section 86E provides lawful authority to disclose personal information where a law that regulates the disclosure of personal information (privacy or secrecy laws) permits disclosure of personal information when 'authorised by law'.

Section 86E provides lawful authority to disclose personal information for the purposes of all Commonwealth, state and territory privacy laws. This is because all Commonwealth, state and territory privacy laws contain an exemption permitting disclosure of personal information where it is 'authorised by law' (section 86E provides this lawful authority).

Section 86E also provides lawful authority to disclose personal information under specific secrecy laws that contain exemptions or exceptions permitting information to be disclosed as 'authorised by law'. It is important to note that section 86E does not apply to some Commonwealth, state and territory secrecy laws which do not contain any 'as authorised by law' exception or exemption. Part VIID does not override those secrecy laws, and cannot be relied upon as authority to disclose personal information which is protected by them.

Further information about lawful authorisation exemptions in state and territory privacy laws is available at *Appendix A.*

Reasonable belief

The person or entity disclosing the information must have a reasonable belief that the personal information is related to one or more of the target entity's functions or activities. As detailed in the definitions section, this requires the entity to have an objectively reasonable basis for its belief, and not merely a genuine or subjective belief.

For example, if an entity receives a letter from the target entity requesting information for an integrity purpose which is relevant to the target entity's functions or activities, this would generally be sufficient for the disclosing entity to form the necessary reasonable belief. Alternatively, the disclosing entity may form the reasonable belief independently based on its knowledge of the target entity's functions and activities, and disclose information to the target entity proactively under section 86E.

The onus for establishing reasonable belief is on the person or entity disclosing the information, not the person or entity receiving or requesting the information.

Who can disclose information?

The disclosing person or entity may be a Commonwealth, state or territory agency, private sector entity or an individual.

If the disclosing entity is also a target entity, the disclosure must be made by a person authorised to make disclosures for an integrity purpose. Depending on the type of entity, this authorisation must be given by:

- the accountable authority of the entity (Commonwealth entities)
- the entity or its principal executive (Privacy Act agencies)
- a director of the entity (wholly-owned Commonwealth companies).[5]

Part VIID does not require the authorisation to take any particular form or manner. It is up to the individual agency to implement its own authorisation methods. Authorisations can apply to named persons, specific positions, or classes of employees. Each agency should consider what is appropriate in its own circumstances. It would be beneficial for authorised officers to undertake privacy awareness training.

Note: The authorised officer requirement does not apply to disclosures made by the Australian Federal Police.

If the disclosing agency is a not a target entity, Part VIID does not place any limitations on who may disclose personal information (providing the person, body or authority reasonably believes the information is relevant to the target agency's functions). Non-target entities may need to consider whether any other laws or policies are relevant to who can disclose personal information in such circumstances.

Who can receive information?

Target entities are authorised to receive information. Anyone in the target agency can receive the information – there is no requirement for individual officers to be authorised to receive information under Part VIID.

Section 86E does not authorise disclosures made to state and territory government agencies or to private sector entities.

---

[5] These terms are explained in the definitions section.

A person disclosing personal information to a target entity under section 86E should make reasonable efforts to ensure they are contacting the appropriate area of that entity, to ensure that the information is going to the correct person or mailbox.

Officers who misuse personal information disclosed under Part VIID remain subject to sanctions under existing legislation.

Who can request information?

Section 86E deals with authority to disclose personal information. There is no requirement for anyone to first request the information, which ensures that people can proactively disclose personal information for integrity purposes.

In many cases disclosure under section 86E will occur in response to a request from a target entity. There are no limitations on who can make such a request. A person requesting information is not responsible for determining whether or not the requirements of section 86E would be met in the circumstances. However, as a practical matter, a requesting agency should provide sufficient information to enable the disclosing agency to be satisfied that the personal information is for an integrity purpose and is relevant to the agency's functions. For example, by providing:

- details of the information required
- the integrity purpose it is to be used for
- how the information is relevant to the agency's functions
- a means to confirm the request is legitimate.

Are there limits on how much information can be disclosed?

An entity may disclose any personal information for an integrity purpose providing it reasonably believes the information is related to the target entity's functions or activities. While there is no limit to the quantity of information that can be disclosed, the disclosing entity needs to ensure the reasonable belief that the personal information is for an integrity purpose relevant to the agency's functions applies to all the information disclosed.

Sharing bulk data and data-matching

Part VIID may facilitate the sharing of bulk data in limited circumstances where disclosure of bulk data sets meets the requirements of section 86E. The agency disclosing needs to reasonably believe it is for an integrity purpose relating to functions or activities of the agency receiving the information.

Agencies considering bulk data sharing should also consider whether other legislation is relevant. For example, the *Data-matching Program (Assistance and Tax) Act 1990* sets out specific requirements for data matching between the agencies covered by that Act, and does not expressly recognise disclosures authorised under other Commonwealth laws.

Where an entity discloses personal information to another Commonwealth entity, the disclosing entity should not disclose more personal information than the amount of personal information necessary to achieve the relevant integrity purpose.

Further resources on data matching

The OAIC has produced a set of guidelines for data-matching that falls under the Data-matching Act: *Guidelines for the Conduct of Data-Matching Program*

The OAIC has produced a set of voluntary guidelines that relate to data matching as an administrative tool: *Guidelines on Data Matching in Australian Government Administration*

Further information on data-matching protocol can be found on the *OAIC website.*

The Department of Home Affairs has created the *Data matching better practice guidelines,* which sets out principles to consider in the technical design, build and analysis of data-matching applications.

Relationship between Part VIID and the Australian Privacy Principles

Section 86F clarifies that Part VIID does not impliedly limit other laws (written or unwritten) that authorise collection, use or disclosure of personal information.

Part VIID is relevant to the 'authorised by law' exemptions to APPs 3 and 6. Other APPs continue to apply to how entities handle personal information. In particular, APP 10 (quality of personal information), APP 11 (security of personal information), APP 12 (access to personal information), and APP 13 (correction of personal information) outline obligations regarding usage and safekeeping of personal information and should be followed unless other exceptions apply.

Part VIID also does not alter the permitted general situations in relation to the collection, use or disclosure of personal information under section 16A of the Privacy Act. This includes where:

- the entity has reason to suspect that unlawful activity, or misconduct of a serious nature, that relates to the entity's functions or activities has been, is being or may be engaged in, and
- the entity reasonably believes that the collection, use or disclosure is necessary in order for the entity to take appropriate action in relation to the matter.

Ensuring procedural fairness

Procedural fairness traditionally involves two requirements: the hearing rule and the bias rule.

- The hearing rule requires a decision-maker to afford a person an opportunity to be heard before making a decision affecting their interests.
- The bias rule ensures that the decision maker can be objectively considered to be impartial and to not have pre-judged a decision.

Target entities must ensure that procedural fairness is considered prior to making any adverse decisions using information gathered under the Part VIID.

What can happen if procedural fairness is not observed?

If procedural fairness is not observed, a person or organisation may be able to take legal action against the decision-maker. A person or organisation may seek judicial review of an administrative decision on the basis that procedural fairness has not been observed. Depending on the legislation under which a decision was made, a person may also be entitled to seek merits review.

Further resources on procedural fairness

The Administrative Review Council's Best Practice Guide has further information on procedural fairness here: *ARC Best Practice Guide 2 - Natural Justice.*

An example of procedural fairness guidelines applying to data-matching can be found in section 5 of the *Guidelines for the Conduct of Data-Matching Program.*

Case studies

The following case studies are taken from real and hypothetical scenarios that have been raised during the development of Part VIID and since its commencement. These case studies are for illustrative purposes only. Entities will need to consider how the legislation applies to their particular situation.

Case study 1 – external disclosure of information about internal frauds

In March 2019 a Commonwealth department made its first disclosure of personal information to a target entity (another government department) for an integrity purpose. The disclosure related to a group of contractors who had previously been engaged by the department and had their contracts cancelled due to inappropriate practices and behaviours. The department became aware that the target entity was in the process of engaging these same contractors.

The department assigned a specific unit to consider and action disclosure requests and proactive disclosures. The unit and the internal investigations section worked together to determine whether the information could be disclosed to the target entity. This included establishing whether the information was personal information or was protected information under other legislation, whether the receiving agency met the definition of a target entity under the Crimes Act and the Privacy Act, and that the target entity's use of the disclosed information would be for an integrity purpose.

The department prepared a formal disclosure document for the target entity, which addressed the key legal provisions of these Acts and only provided sufficient information to assist the target entity undertake their integrity purpose. The disclosure was well received by the target entity.

Case study 2 – member of the public provides personal information to Commonwealth department regarding a potentially fraudulent activity by a service provider

A member of the public provided personal information to a Commonwealth department (Department A) regarding potentially fraudulent activity by a service provider. Department A did not administer that service provider, but held a reasonable belief that the personal information was related to the activities of another target entity Commonwealth department (Department B) who administered the provider.

As Department A was a target entity, disclosure of personal information had to be made by an authorised person, in this case the Secretary. The Secretary was satisfied that the disclosure would be for an integrity purpose of investigating fraud that may have a substantial adverse effect on the Commonwealth. The relevant privacy and secrecy provisions contained 'authorised by law' exemptions, so there was lawful authority for the disclosure. The Secretary was satisfied Department A was providing the information to the correct recipient in Department B, and disclosed the information to them via email.

Department B used the information for the integrity purpose of investigating serious fraudulent behaviour by the service provider. Department B also took administrative action under the relevant legislation by removing the fraudulent service provider, and imposed a financial penalty.

Case study 3 – Employee investigated for fraud seeks employment at another Commonwealth agency

Employee X at Commonwealth Agency A (a non-law enforcement agency) is suspected of committing significant fraud against Agency A. Agency A is finalising their fraud investigation, when Employee X resigns, before the investigation is finalised.

Employee X is successful in obtaining employment with Commonwealth agency B.

Providing no other secrecy laws apply, Part VIID provides lawful authority for Commonwealth Agency A to pass information to Commonwealth Agency B, as preventing Employee X from committing fraud would constitute an integrity purpose. Agency A could pass the information to Agency B either at Agency B's request or of Agency A's own initiative, having formed a reasonable belief that the information may be used for an integrity purpose that is relevant to Agency B's functions. The person from Agency A that discloses the information to Agency B must be authorised by the Secretary of the purpose of Part VIID.

Case study 4 – Commonwealth agency seeks details about a person held by a private entity

Commonwealth Agency A needs employment details of Customer X at Large Company B to investigate an internal fraud. A staff member from Agency A's fraud unit contacts Company B to request these details.

Large Company B, while not compelled to do so, is able to pass personal information to Commonwealth Agency A for the integrity purpose of investigating a fraud, and will not be contravention of privacy laws. The sharing of information for an integrity purpose is authorised under Part VIID, providing that all general privacy principles, secrecy or other applicable laws are also adhered to. Part VIID does not contain any requirements as to who from Agency B may provide the information to Agency A.

Case study 5 – Information obtain under a search warrant

A Commonwealth law enforcement agency executes a search warrant under section 3E of the Crimes Act. Material seized pursuant to the search warrant is supplied to Commonwealth Agency A to support a fraud investigation. Commonwealth Agency A identifies that personal information obtained under the search warrant is indicative of fraud against Commonwealth Agency B and Company C, an insurance company.

Agency A wants to be proactive and provide the information gathered from the search warrant to Agency B and Private Company C to assist the prevention, detection, investigation or to otherwise deal with the fraud, and consults its internal legal area for advice on whether it can do so.

Part VIID provides authorisation for Commonwealth Agency A to disclose information to Commonwealth Agency B. This will not breach the Privacy Act as information is being passed for an integrity purpose, providing general privacy principles and secrecy laws are also adhered to.

In relation to Company C, Part VIID does not provide authorisation for information to be disclosed by Agency A to Company C, as Company C is not a target entity.

Note: this example could also apply where information was legally gathered under a state or territory search warrant and disclosed to a Commonwealth agency for an integrity purpose.

Case study 6 – Agency seeks information protected under a secrecy provision

Commonwealth Agency A needs personal information about Person X, held by Agency B, to investigate a fraud against Agency A. A fraud investigator from Agency A phones their contact in Agency B's fraud team to ask if Agency B can provide the personal information for Agency A's integrity purpose.

Agency B will need to consider whether the secrecy provisions contain an exemption permitting it to disclose the information to Agency A. Agency B will also need to ensure compliance with the requirements of Part VIID. Agency B may wish to consider seeking legal advice on the interaction between its specific secrecy provisions and Part VIID.

Appendix A: State and Territory Privacy Laws

Appendix A outlines key clauses in state and territory privacy laws which regulate the collection, use and disclosure of personal information. Please note that this list does not purport to be a comprehensive list of all potentially relevant legislation.

Australian Capital Territory

The *Information Privacy Act 2014* (ACT) regulates the handling of personal information by ACT public sector agencies.

Section 3.4(a) in Part 1.2 of the Act allows collection of sensitive information as authorised by or under an Australian law.

Section 6.2(b) in Part 1.3 of the Act allows use and disclosure of personal information as required or authorised by or under an Australian law.

New South Wales

The NSW Information and Privacy Commission undertakes the privacy functions conferred by the *Privacy and Personal Information Protection Act 1998* (NSW) and *Health Records and Information Privacy Act 2002* (NSW).

Section 25 of the *Privacy and Personal Information Protection Act 1998* (NSW) allows the collection, use and disclosure of personal information if:

- the agency is lawfully authorised or required not to comply with the principle concerned, or
- non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).

The Health Privacy Principles (HPPs) are contained in Schedule 1 of the *Health Records and Information Privacy Act 2002* (NSW). HPPs 10.2 and 11.2 authorise organisations to use and disclose health information if the organisation is lawfully authorised.

Northern Territory

The Office of the Information Commissioner for the Northern Territory is the independent statutory body responsible for overseeing the privacy provisions of the *Information Act 2002* (NT). The Information Privacy Principles (IPPs) are contained in Schedule 2 of the Act.

IPP 2.1(f) in Schedule 2 of the Act allows the use and disclosure of personal information if required or authorised by law.

IPP 9.1(a) in Schedule 2 allows the transfer of personal information about an individual to a person outside the Territory if the transfer is required or authorised under a law of the Territory or the Commonwealth.

IPP 10.1(b) in Schedule 2 allows a public sector organisation to collect sensitive information about an individual if authorised or required by law.

Queensland

The Queensland Office of the Information Commissioner receives privacy complaints under the *Information Privacy Act 2009* (Qld) which covers the Queensland public sector. The IPPs are contained in Schedule 3 of the Act. The National Privacy Principles (NPPs) are contained in Schedule 4 of the Act.

IPP 11(d) in Schedule 3 allows an agency to disclose a document containing an individual's personal information to an entity, other than the individual subject of the personal information, if authorised or required by law.

NPP 2(1)(f) in Schedule 4 allows a health agency to disclose personal information for a purpose other than the primary purpose of collecting if authorised or required by or under law.

South Australia

South Australia has issued an administrative instruction requiring its government agencies to generally comply with a set of Information Privacy Principles and has established a South Australian privacy committee to handle privacy complaints.

IPP (10)(d) allows for the disclosure of personal information to a third person for a purpose that is not the purpose of collection if required or authorised by or under law.

Tasmania

The Tasmanian Ombudsman may receive and investigate complaints in relation to the *Personal Information and Protection Act 2004* (Tas). This legislation covers the Tasmanian public sector including the University of Tasmania. The Personal Information Protection Principles (PIPPs) are contained in Schedule 1 of the Act.

PIPP 2(1)(f) allows for the use and disclosure of personal information about an individual for a purpose other than the purpose for which it was collected if required or authorised by or under law.

PIPP 9(e) allows the disclosure of personal information to another person or another body who is outside Tasmania if authorised or required by any other law.

Victoria

The Office of the Victorian Information Commissioner (OVIC) was established on 1 September 2017 and consists of the Information Commissioner, the Public Access Deputy Commissioner, the Privacy and Data Protection Deputy Commissioner and their staff. The *Freedom of Information Act 1982* (Vic) sets out the powers and functions of the Information Commissioner and the Public Access Deputy Commissioner in relation to Freedom of Information.

The *Privacy and Data Protection Act 2014* (Vic) sets out the powers and functions of the Information Commissioner and the Privacy and Data Protection Deputy Commissioner in relation to information privacy, protective data security and law enforcement data security. The IPPs are contained in Schedule 1 of the Act.

IPP 2.1(f) in Schedule 1 allows for the use or disclosure of personal information about an individual for a purpose other than the primary purpose of collection if required or authorised by or under law.

The HPPs are contained in Schedule 1 of the *Health Records Act 2001* (Vic).

HPP 2.2(c) in Schedule 1 allows an organisation to use or disclose health information about an individual for a purpose other than the primary purpose for which it was collected if the use or disclosure is required, authorised or permitted, whether expressly or impliedly, by or under a law.

HPP 9.1(g) in Schedule 1 allows for the *transfer* of health information to someone who is outside Victoria only if the transfer is authorised or required by any other law.

Western Australia

The state public sector in Western Australia does not currently have a legislative privacy regime. Various confidentiality provisions cover government agencies and some of the privacy principles are provided for in the *Freedom of Information Act 1992* (WA) overseen by the Office of the Information Commissioner (WA).

The current guidance provided by the WA Government on privacy legislation is as follows:

> *Until such time as more substantial guidance and/or legislative measures are available, the interim privacy position for the Western Australian public sector is that agencies should ensure their actions are consistent with applicable Australian Privacy Principles, set out in Schedule 1 to the Privacy Act 1988 (Cth) with primary emphasis upon Principle 6 - "use or disclosure of personal information".*