

**UNDERSTANDING CULTURALLY DIVERSE PRIVACY**

**Aboriginal and Torres Strait Islander peoples’ perspectives**

**The Office of the Victorian Information Commissioner acknowledges the Aboriginal Traditional Owners of Country throughout Victoria and pays respect to their cultures and Elders past, present and emerging.**

**The artwork by Jordan Lovegrove, a Ngarrindjeri man of Dreamtime Creative, shows OVIC protecting information rights for different people and communities. The large central meeting place represents OVIC while the smaller meeting places around the outside show the different communities. The dotted pathways and the dots in the centre represent OVIC protecting communities information.**

**CONTENTS**

[INTRODUCTION 4](#_Toc69563105)

[Purpose of this resource 4](#_Toc69563106)

[Context 4](#_Toc69563107)

[CIRCA RESEARCH AND FINDINGS 5](#_Toc69563108)

[Scope and methodology 5](#_Toc69563109)

[Key findings – collection of personal information 6](#_Toc69563110)

[Key findings – use and disclosure of personal information 6](#_Toc69563111)

[Key findings – trust in organisations 7](#_Toc69563112)

[PRIVACY CONSIDERATIONS 7](#_Toc69563113)

[Collection of personal information 7](#_Toc69563114)

[Use and disclosure of personal information 8](#_Toc69563115)

[Data quality 10](#_Toc69563116)

[Transparency 10](#_Toc69563117)

[Consent 10](#_Toc69563118)

[BUILDING TRUST 11](#_Toc69563119)

[Consultation and community control 12](#_Toc69563120)

[Effective communication 12](#_Toc69563121)

[Seeking consent 13](#_Toc69563122)

[Organisational reform and a human centred approach 13](#_Toc69563123)

[CONCLUSION 14](#_Toc69563124)

INTRODUCTION

Privacy is a complex concept, encompassing many interrelated ideas and influenced by factors such as age, background and culture.[[1]](#endnote-1) It is also not a fixed concept; different people and different groups will experience, understand, and value privacy in varied ways, which can change over time.

One dimension of privacy is the notion of control over one’s personal information. Commonly referred to as information privacy, this relates to an individual’s ability to determine when, how, and for what purpose their personal information is used. Many privacy laws, including Victoria’s *Privacy and Data Protection Act 2014* (**PDP Act**), regulate information privacy and the protection of personal information.[[2]](#endnote-2)

In Victoria, privacy is also a human right enshrined in the *Charter of Human Rights and Responsibilities Act 2006* (**the Charter**), which requires Victorian public authorities to consider how privacy is protected when creating legislation, implementing policies, or delivering services.[[3]](#endnote-3) The right to privacy under the Charter is broader than the concept of information privacy, referring to an individual’s right not to have their privacy, family life, home or correspondence (such as mail or email) interfered with.

The right to privacy (both in terms of information privacy and privacy more broadly) as protected under the PDP Act and the Charter respectively, focuses on the rights of individuals. But privacy can also be conceived as a group right, rather than an individual right alone. For example, some groups or cultures – such as Indigenous groups – may focus on collective rights in relation to information, and a privacy interest may affect not only the individual to whom the information relates, but also the wider group to which the individual may belong.[[4]](#endnote-4)

Further, while the PDP Act and other privacy laws define what constitutes personal information, different groups and individuals may have varying views around what they consider to be personal (and sensitive)[[5]](#endnote-5) information, which may not necessarily align with the definitions under privacy legislation.

Purpose of this resource

As the primary regulator for information privacy in Victoria with administration over the PDP Act, the Office of the Victorian Information Commissioner (**OVIC**) seeks to better understand how different cultures perceive information privacy, in particular Aboriginal and Torres Strait Islander communities in Victoria. Gaining an awareness and understanding of different cultural attitudes towards information privacy may help to address some of the barriers and challenges to the collection, use and disclosure of personal information of individuals from different backgrounds.

This resource draws on the findings of research conducted by the Cultural and Indigenous Research Centre Australia (**CIRCA**) for OVIC between April and June 2020. It will outline potential considerations for the Victorian public sector (**VPS**) when collecting, using and disclosing Aboriginal and Torres Strait Islander peoples’ personal information, with reference to the PDP Act. OVIC hopes that this resource will give an insight into Aboriginal and Torres Strait Islander perspectives towards the handling of personal information and provide a starting point for discussion into cultural privacy.

Context

In 2002, the former Office of the Victorian Privacy Commissioner published a report, *Privacy in diverse Victoria* (**OVPC report**), which looked at attitudes towards information privacy amongst culturally and linguistically diverse communities and Indigenous groups in Victoria.[[6]](#endnote-6) The report noted several issues raised by Indigenous individuals, including:

* concerns around the overcollection and sharing of personal information;
* concerns around personal information being misused against the individual, and incorrect information being held by the collecting organisation;
* a desire for control when personal information is shared – for example, knowing why the information is being collected, how it will be used, and having the ability to provide consent and check the accuracy of the information being shared; and
* accepting the ‘inevitable’ sharing of personal information, if it benefits the community or individual; for example, if the sharing helps to protect children.

Since the release of this report, little to no further research has been conducted in Victoria into Aboriginal and Torres Strait Islander peoples’ attitudes towards information privacy.

Elsewhere, the Australian Law Reform Commission’s (**ALRC**) 2008 report *For Your Information: Australian Privacy Law and Practice* explored the privacy of Indigenous groups, and the idea of privacy protocols to protect those groups’ privacy rights.[[7]](#endnote-7)

The use of a privacy protocol to assist organisations in addressing the particular privacy needs of Indigenous groups (and other ethnic or cultural groups) is not new. In 1998 the federal Office of the Privacy Commissioner developed a privacy protocol to assist Commonwealth agencies handling the personal information of Indigenous people in the Northern Territory.[[8]](#endnote-8)

The protocol aimed to provide an interpretation of some aspects of the Information Privacy Principles under the federal *Privacy Act 1988* in a way that was culturally appropriate for Aboriginal and Torres Strait Islander people in the Northern Territory. For example, it listed examples of culturally sensitive information, disclosure of personal information to third parties, and issues relating to the collection of personal information.

CIRCA RESEARCH AND FINDINGS

OVIC’s aim in commissioning the CIRCA research was to gain a better understanding of Aboriginal and Torres Strait Islander peoples’ attitudes towards information privacy – specifically, their views on the cultural appropriateness of certain practices relating to the collection, use and disclosure of personal information. The research was limited to Aboriginal and Torres Strait Islander peoples living in Victoria (noting the diversity of communities, cultures and languages within the state).[[9]](#endnote-9)

Scope and methodology

CIRCA’s research focused on the collection, uses, and disclosures of personal information and, through the use of hypothetical scenarios, whether certain practices were considered to be culturally inappropriate or insensitive. The research also looked at ideas for building trust in organisations’ collection and handling of the personal information of Aboriginal and Torres Strait Islander individuals.

As part of the research, CIRCA conducted focus group interviews with a diverse mix of 12 Aboriginal participants living in Victoria. Given the small sample size, the findings are not representative of the views of all Aboriginal or Torres Strait Islander individuals. Nonetheless, the research identifies important themes and privacy considerations for organisations collecting and handling the personal information of Aboriginal and Torres Strait Islander peoples – and, indeed, the broader community.

Additionally, as the PDP Act protects the information privacy rights of individuals, it should be noted that CIRCA’s research focuses only on individual rights in relation to privacy and personal information. However, as noted above, some cultures – including Aboriginal and Torres Strait Islander cultures – may consider certain types of information as belonging to the group rather than to individuals, and as such may place a greater emphasis on collective, versus individual rights.[[10]](#endnote-10)

Key findings – collection of personal information

CIRCA’s research identified several issues raised by Aboriginal participants in relation to the collection of personal information. In particular, participants had concerns with being asked to provide personal information of individuals other than themselves to government organisations.

Participants reported that they would be uncomfortable providing personal information about other individuals (for example, family members) to organisations requesting this data, citing reasons such as consent not having been provided by that other individual, and that individual not being able to be informed about how their information will be used.

Notably, some participants also raised cultural concerns around the provision of information about other individuals:

“…it’s not culturally appropriate to share personal information of our Elders or peers…with people outside our immediate or even part extended family… So even if it was a community organisation you trusted or a completely different organisation, it’s still culturally inappropriate to share more than basic information to anyone outside the family.”

The research also asked participants about methods of data collection. While there was no particular method considered to be more culturally appropriate or inappropriate than others, participants noted their preferred method of collection depends on the context and circumstances. In the hypothetical scenario of applying for a government service, some participants preferred the convenience of online collection, while others noted technological literacy, the ability to build a relationship with the organisation, and being able to interact with a person with an awareness of Aboriginal people and their culture as reasons for preferring an in-person collection of their personal information.

Key findings – use and disclosure of personal information

In terms of use and disclosure of personal information, most participants expressed being unhappy in the hypothetical scenario of an organisation using personal information held about them for a secondary use other than the original purpose of collection, even where the secondary use or disclosure was legitimate or legally permitted:

“I feel the data you provide should only be used for the purpose you originally provided it for, not so that [they] can re-use the data.”

The need for consent was raised, particularly in the context of disclosure of personal information to other organisations. Being informed about the purpose for disclosure was also important to participants. One participant noted:

“…some [information] you felt you could share with [one] agency you would not share [with the other] due to cultural reasons”

Some participants raised the issue of trust in an organisation, and how this could be eroded where disclosure of their personal information to a third party occurred without their consent or knowledge.

Key findings – trust in organisations

CIRCA’s research identified several key issues in relation to trust in organisations’ collection and handling of personal information. Aboriginal participants who participated in the research cited a number of different reasons for distrust in organisations, such as:

* colonisation and historical injustices;
* a lack of transparency;
* power imbalances (between the organisation collecting the data and the Aboriginal and Torres Strait Islander peoples from whom the data is collected); and
* organisations not adequately accommodating for the needs of Aboriginal and Torres Strait Islander peoples.

“A high percentage of government [organisations] and community services don’t actually have any culturally appropriate processes in place to share sensitive information about, for, and on behalf of Aboriginal people”

The research sought participants’ views on how organisations could build trust with Aboriginal and Torres Strait Islander peoples. Several ways to enhance trust were identified, which are outlined in Section 4.

PRIVACY CONSIDERATIONS

This section considers privacy considerations in relation to the Information Privacy Principles (**IPPs**) under the PDP Act, in light of the findings summarised in Section 2 above.[[11]](#endnote-11) The IPPs provide a minimum standard for the collection, storage, handling and disposal of personal information held by VPS organisations.[[12]](#endnote-12)

Collection of personal information

IPP 1 (Collection) outlines a number of requirements for organisations when collecting personal information. For example:

* it must be necessary for one or more of an organisation’s functions or activities (IPP 1.1);
* the collection must be lawful, fair, and not unreasonably intrusive (IPP 1.2);
* organisations must take reasonable steps to provide individuals with certain details about the collection (IPP 1.3); and
* where reasonable and practicable, organisations must collect personal information directly from the individual (IPP 1.4).

**Direct vs indirect collection**

IPP 1.4 requires organisations, where reasonable and practicable, to collect personal information about an individual only from that individual. Collecting personal information directly ensures that individuals are aware of the collection, and provides them with control over what is collected, by whom and for what purpose.

The importance of individuals being aware of the collection of their personal information was raised in CIRCA’s research, along with their being informed of the purposes for which the information will be used or disclosed.

Organisations have an obligation under IPP 1.5 to take reasonable steps to provide a notice of collection where personal information is collected indirectly, but in cases of indirect collection individuals are not given the opportunity to refuse collection, or provide consent for certain uses or disclosures, which, as will be explored further in this resource, is an important issue identified by many participants.

Collecting personal information directly from individuals can help to ensure that the information is accurate, complete and up to date. On the other hand, indirect collection raises the risk that personal information collected from a source other than the relevant individual is incomplete or out of date. For example, collecting personal information indirectly from publicly available sources such as social media poses the risk that the information is inaccurate or no longer up to date. Individuals may also not be aware that personal information is being collected from their social media, and therefore do not have the opportunity to refuse the collection or provide accurate details.

Indirect collection could also potentially lead to organisations inadvertently collecting information that may not be considered culturally appropriate to share with that organisation.

**Sensitive information**

The PDP Act lists nine categories of sensitive information, including information relating to an individual’s racial and ethnic origin. IPP 10 (Sensitive Information) places greater limitations around the collection of sensitive information, which acknowledges that this type of information carries inherent risks to individuals’ privacy and other rights. For example, one risk commonly associated with the collection and handling of sensitive information is discrimination on the basis of racial or ethnic origin, political opinions, or sexual practices.

Many organisations commonly collect information about racial or ethnic origin (for example, identification or status as an Aboriginal or Torres Strait Islander person) for purposes such as providing community-specific services or recruitment for a designated role. However, Aboriginal and Torres Strait Islander individuals may be reluctant to provide this type of sensitive information for reasons such as historical and contemporary experiences of racism and discrimination, fear of negative consequences, uncertainty and mistrust about why the information is being collected and how it will be used, and cultural stereotyping.[[13]](#endnote-13)

The Australian Bureau of Statistics’ (**ABS**) 2014 Review of the Indigenous Status Standard (the basis for the ABS and many other organisations’ collection of Aboriginal and Torres Strait Islander statistics) found that a lack of understanding around why information about Indigenous status is collected and what the data is used for can lead to an unwillingness to provide this information.[[14]](#endnote-14) Further, the ABS noted that ‘understanding why the data is collected strongly correlates with higher levels of compliance and improved data quality’.[[15]](#endnote-15)

Providing individuals with adequate details about why Aboriginal or Torres Strait Islander identification is being collected and what it will be used for is essential to individuals’ ability to give informed, meaningful consent, which is commonly relied upon as the basis for collecting sensitive information under IPP 10.

Use and disclosure of personal information

Under the PDP Act, organisations must not use or disclose personal information for a purpose other than the original purpose of collection, unless an exception under IPP 2 applies.

These exceptions include:

* where the secondary use or disclosure is related to the primary purpose of collection and is reasonably expected by the individual (IPP 2.1(a));
* with the consent of the individual (IPP 2.1(b)); or
* where the use or disclosure is required or authorised by or under another law (IPP 2.1(f)).

**Consent**

While consent is only one of the legal bases under which organisations can use or disclose personal information for a secondary purpose under the PDP Act, many Aboriginal participants who took part in CIRCA’s research placed great value on consent and having the ability to control the use and disclosure of their personal information, even in circumstances where its secondary use or disclosure would have been permitted without consent.

“Without consent or prior knowledge, I always have a problem with data sharing. The benefit of any data sharing is outweighed by people’s right to privacy and control over their own data.”

When relying on individuals’ consent to use or disclose their personal information, consent must be meaningful. This can be challenging, as discussed further in Section 3.5 below.

**Reasonably expected**

Another common basis for secondary use or disclosure of personal information is where it is related to the primary purpose of collection, and is reasonably expected by the individual. Whether a use or disclosure is ‘reasonably expected’ depends on what an ordinary person would consider reasonable in the particular circumstances (rather than the expectation of the actual individual concerned). What an ordinary person would consider reasonable can be influenced by a range of factors, including the nature of the organisation, the sensitivity of the information, and the individual’s expressed expectations.[[16]](#endnote-16)

Community expectations can also play an important role in determining what is considered reasonable in the particular circumstances. Victoria has diverse Aboriginal and Torres Strait Islander communities, whose expectations around how personal information should be used and disclosed, and views around what uses or disclosures are culturally acceptable or inappropriate, may differ across communities. This is reflected in one Aboriginal participant’s comment which, while related to collection, is nonetheless relevant in the context of use and disclosure:

“Data collection could be made more culturally appropriate by not expecting all Indigenous peoples to fit in one box.”

Another factor that can influence reasonable expectations is the notice provided to the individual upon collection of their personal information. Under IPP 1.3, organisations are required to take reasonable steps to make individuals aware of certain information (often referred to as a collection notice), including the purposes for which their personal information is collected, and organisations or individuals to whom that information is usually disclosed. A good collection notice can set up an individual’s expectations about how their personal information will be used and disclosed, as required under IPP 2.1(a).

Data quality

IPP 3 (Data Quality) requires VPS organisations to take reasonable steps to ensure the personal information they collect, use or disclose is accurate, complete, and up to date. Ensuring the data quality of personal information is important, as personal information is often used to make decisions that affect communities and individuals’ lives. For example, an incorrect age can affect an individual’s concession entitlements, or inaccurate personal information about an individual involved in an investigation can cause serious harm.

Collecting personal information directly from an individual (compared to indirect collection) is one way to ensure the quality of the information. Several studies and best practice guidelines (largely within the context of health service provision) have noted self-identification (also self-reporting) as the most accurate means of ascertaining an individual’s Aboriginal or Torres Strait Islander status – as opposed to the data collecting organisation making an assumption based on factors such as appearance or language, and recording this assumption on the individual’s behalf.[[17]](#endnote-17)

Taking reasonable steps to check that such information is up to date before it is used or disclosed is also important, particularly as individuals may choose to identify or not identify as Aboriginal or Torres Strait Islander at different stages of their life. Providing individuals with the opportunity to confirm or amend this information (as well as other categories of their personal information) is therefore essential for ensuring data quality under IPP 3.

Transparency

Transparency about organisations’ use and disclosure of personal information was a major theme identified in CIRCA’s research, with Aboriginal participants frequently highlighting the importance of being aware of the purposes for which their personal information would be used, particularly in the context of secondary use or disclosure to third parties.

“…when we give [information] to government they tell us how it will be used, but I feel we never really know what else it is being used for. Government agencies share information all the time and I feel this is not explained to people enough.”

Being transparent about secondary uses or disclosures of personal information can help promote trust and accountability. It can also help foster a positive relationship between the organisation and individual or community, which can be valuable for public acceptance of new programs or projects involving the use of personal and sensitive information. Additionally, as noted above, being transparent about how personal or sensitive information will be used or disclosed can help ensure the quality of data being collected, as individuals are more likely to share accurate information about themselves if they are comfortable with how it will be used and shared.

This principle of transparency underpins IPP 5 (Openness), which requires organisations to set out their policies on the management of personal information in a publicly available document, often referred to as a privacy policy.

Consent

Consent is a fundamental concept underpinning many privacy laws, including the PDP Act. In the context of information privacy, consent refers to the ability of individuals to make choices (in certain circumstances) about when and how their personal information is collected and used.

While consent is only one basis among many that organisations can rely on to use or disclose personal information for a secondary purpose, CIRCA’s research demonstrated that for the Aboriginal participants, being able to control how their information is used and shared, through the provision of consent, is essential.

“I wouldn’t appreciate my data being shared without my permission, or someone contacting me for their own purpose, not for my actual benefit.”

However, consent should be meaningful. Meaningful consent has five elements: it must be informed, voluntary, current, specific, and given by an individual with capacity to agree with what is being asked of them.[[18]](#endnote-18) For example, for consent to be voluntary, individuals must be able to exercise genuine control. Seeking consent for a secondary use or disclosure that is permitted under a law, and which will occur irrespective of whether consent is given or not, may seem disingenuous, and the consent will likely be invalid. Similarly, consent will likely not be voluntary where the provision of consent is conditional to accessing a service, or an organisation seeks consent for the collection of sensitive information it is legally permitted to collect without consent.

Another element that is particularly relevant in light of CIRCA’s research is that consent must be informed. This involves individuals knowing all the relevant facts, including who their information will be shared with and what it will be used for. Importantly, informed consent depends on the individual understanding the information presented to them, taking into account any particular vulnerabilities. For example, providing information about how personal information will be used does not necessarily mean the individual will understand that information. Individuals’ literacy levels may vary, which can impact on their understanding of how their personal information will be used and disclosed. Similarly, framing information in a way that individuals are not familiar with – such as using highly technical or legal language – may also impact on individuals’ ability to provide informed consent. This is reflected in one Aboriginal participant’s comment, in relation to challenges in communicating with organisations about data collection and use practices:

“Jargon is a major factor. It’s not clearly written for many to understand, and many people just sign up for things without knowing the consequences.”

This ties into another element of consent: capacity. An individual may not be capable of providing consent due to factors such as cultural and linguistic differences, and level of literacy, including digital literacy.

BUILDING TRUST

Trust is essential for government to be able to build and maintain legitimacy and acceptance from the public to collect and use citizens’ personal information, deliver good services, and develop a positive relationship with its citizens. Building trust in the collection, use and disclosure of Aboriginal and Torres Strait Islander peoples’ personal information is particularly important, given the historical and ongoing injustices and misuses of personal information experienced by individuals in those communities.

While compliance with privacy laws is crucial, CIRCA’s research demonstrates that this is only one element of a broader strategy needed to foster trust in an organisation’s collection and handling of Aboriginal and Torres Strait Islander peoples’ personal information. Aboriginal participants in CIRCA’s research identified several other essential elements to help build trust.

Consultation and community control

Participants noted the importance of genuine and respectful consultation with Aboriginal and Torres Strait Islander communities on matters relating to their information privacy, and allowing input into how their personal information is used. Noting the diversity and complexity of Aboriginal and Torres Strait Islander communities, consultation can be valuable for ensuring the use of personal information aligns with community expectations. It also plays an important role in fostering public acceptance and uptake of programs involving personal information and can help build trust in organisations’ use of personal information.

Another suggestion provided by participants was community control, which goes beyond consultation to empower and enable Aboriginal and Torres Strait Islander communities to handle and make decisions about their own personal information. Community control allows Aboriginal and Torres Strait Islander communities to be involved in their own affairs in accordance with protocols or procedures determined by the community,[[19]](#endnote-19) and is closely tied to the notion of Aboriginal self-determination (broadly, the right for Aboriginal peoples to make decisions on matters that affect their lives and communities).

This need for community control of data is recognised in the Victorian Government’s *Victorian Aboriginal Affairs Framework 2018-2023*, which is underpinned by the principle of Aboriginal self-determination: “…increasing Aboriginal ownership and control of data is a key enabler of self-determination”.[[20]](#endnote-20) As one Aboriginal participant reflected:

“While data may be used to develop policies to assist mob, I have real issues with who is developing those policies and who has ownership of the data that is collected… Now more than ever Government should be helping to fund Aboriginal [organisations] to do the work and store the data so there is oversight by mob of how it is used.”

Effective communication

Communicating effectively with individuals about information privacy matters can be a challenge for many organisations. For example, privacy policies – which are a key source of information about how an organisation uses and discloses personal information – are often lengthy, complex and difficult to understand, and few individuals meaningfully engage with them.[[21]](#endnote-21) This issue of effective communication is crucial as it has implications for consent – if individuals cannot fully understand how their personal information will be used, they are unlikely to be able to provide informed, meaningful consent.

The importance of effective communication was identified by many Aboriginal participants in CIRCA’s research, along with the need to use different approaches to cater to different levels of education and literacy, and tailoring the communication for the specific audience; for example:

* minimising jargon;
* using infographics to assist with understanding; and
* framing issues in culturally appropriate language that Aboriginal and Torres Strait Islander people can better relate to.[[22]](#endnote-22)

The need for more support and education for Aboriginal and Torres Strait Islander individuals regarding privacy matters was also identified, with one participant noting:

“I think not enough education is provided to community using services and their rights of information privacy and data collection when using such services… Educate our people; don’t hide it in the signing of documents.”

These issues were similarly raised in the ABS’ research exploring perspectives on Aboriginal and Torres Strait Islander identification, which raised literacy and language as one factor in individuals’ tendency to identify as Indigenous; in particular, the ABS noted the need to provide support to those who require assistance with reading forms or understanding questions in English.[[23]](#endnote-23) In its report *Strangers in their own land: Use of Aboriginal Interpreters by NT public authorities*, the Ombudsman NT cautioned against overestimating individuals’ English proficiency and noted that ultimately, organisations have a responsibility to ensure effective communication. The report states that ‘ensuring effective communication may be complicated by a range of cultural and social factors… but these complications are for the agency to recognise and manage’.[[24]](#endnote-24) The use of Aboriginal interpreters (the topic of the NT Ombudsman’s report) in appropriate circumstances may be one strategy to enable organisations to better communicate with individuals about privacy matters.

Seeking consent

Control over personal information and how it is used and disclosed, through the provision of consent, is a consistent theme raised by participants throughout CIRCA’s research. Participants noted the need for such consent to be informed, and for individuals providing it to fully understand what they were consenting to. As noted above, while it is not feasible in all circumstances to seek consent, and obtaining meaningful consent can be challenging, doing so where practicable can foster trust between organisations and Aboriginal and Torres Strait Islander peoples, with consent raised by participants as one strategy for building trust.

Organisational reform and a human centred approach

“To be more culturally sensitive, organisations need to have an understanding of issues that Indigenous people face regularly, and be respectful and mindful of how systems affect us.”

The need for reform to promote and ensure culturally safe and inclusive services was noted by participants as another way for organisations to foster trust. Collecting data from Aboriginal and Torres Strait Islander people in a respectful and sensitive way could also enhance individuals’ willingness to provide personal information voluntarily, as well as improve data quality.

The Victorian Family Violence Data Collection Framework describes cultural safety as an environment ‘where services are provided in a manner that is respectful of a person’s culture and beliefs, and that is free from discrimination’.[[25]](#endnote-25) Ensuring a culturally safe environment requires organisations to analyse their organisational culture and ensure that it does not have a negative impact on the cultural rights of Aboriginal and Torres Strait Islander communities. This may involve examining policies and processes to ensure they are inclusive of Aboriginal and Torres Strait Islander people, providing cultural awareness training to staff, and accommodating the needs of Aboriginal and Torres Strait Islander communities.

Some examples given by participants included:

* tailoring services specific to “men’s and women’s” business;
* adopting a more personalised approach towards data collection that builds trust, rather than treating individuals as simply a ‘number’ – for example, face to face interaction with communities;
* providing the option to deal with Aboriginal liaison officers; and
* recognising the diversity of Aboriginal and Torres Strait Islander communities, rather than a one size fits all approach.

The importance of cultural awareness on the part of organisations collecting data was also recognised in previous research conducted by the ABS, as a key factor in improving Aboriginal and Torres Strait Islander identification. The attitude of data collection staff was also highlighted; that is, ‘the need for staff to understand, and be able to explain, the reason for collecting the data’, as well as ‘the need for a positive interaction around identification’.[[26]](#endnote-26)

CONCLUSION

A better understanding of different cultural perspectives around the collection, use and disclosure of personal information is essential for promoting a culturally sensitive and appropriate approach towards the handling of such information, in addition to complying with Victorian privacy laws. Handling personal information in a culturally safe manner has benefits for both individuals and organisations alike – such as enhancing trust, improving data quality, and improved understanding about how personal information will be used.

OVIC encourages VPS organisations to consider the issues discussed in this resource and think about ways to make their processes for the collection and handling of personal information more culturally sensitive.

Finally, OVIC would like to thank CIRCA for their research, and the participants who took part for their time.

1. For example, the Australian Law Reform Commission’s report *For Your Information: Australian Privacy Law and Practice* (ALRC Report 108, 2008) outlines different elements of privacy [at 1.31] including *bodily privacy*, which is described as concerning the “protection of people’s physical selves against invasive procedures such as genetic tests, drug testing and cavity searches”. Another element is *territorial privacy*, defined as concerning “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”. [↑](#endnote-ref-1)
2. Personal information is defined under section 3 of the PDP Act as ‘information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can be reasonably ascertained, from the information or opinion’. This definition excludes health information, which is regulated under the *Health Records Act 2001* (Vic). [↑](#endnote-ref-2)
3. Section 13 of the Charter. For more information see the Victorian Equal Opportunity and Human Rights Commission’s website at <https://www.humanrights.vic.gov.au/for-individuals/human-rights/>. [↑](#endnote-ref-3)
4. See section 7 of the ALRC Report 108 (2008), ‘Privacy Beyond the Individual – Privacy and group rights generally’. [↑](#endnote-ref-4)
5. Sensitive information is a subset of personal information, and is defined in Schedule 1 of the PDP Act. [↑](#endnote-ref-5)
6. Office of the Victorian Privacy Commissioner, *Privacy in* diverse *Victoria*, October 2002. [↑](#endnote-ref-6)
7. See ALRC Report 108, section 7 ‘Privacy Beyond the Individual’, available at <https://www.alrc.gov.au/publication/for-your-information-australian-privacy-law-and-practice-alrc-report-108/7-privacy-beyond-the-individual/>. [↑](#endnote-ref-7)
8. Office of the Privacy Commissioner, *Minding Our Own Business: Privacy Protocol for Commonwealth Agencies in the Norther Territory Handling Personal Information of Aboriginal and Torres Strait Islander People*, February 1998. [↑](#endnote-ref-8)
9. When referring to the CIRCA research this resource will use the term ‘Aboriginal’ given the demographic of the participants; however, when referring to ‘Aboriginal and Torres Strait Islander groups’ in general this collective term will be used. [↑](#endnote-ref-9)
10. Aboriginal Privacy Project Insights Report, Cultural and Indigenous Research Centre Australia, 1 July 2020. [↑](#endnote-ref-10)
11. The IPPs can be found under Schedule 1 of the PDP Act. They apply to Victorian public sector organisations covered by Part 3 of the PDP Act, as listed under section 13 of the Act. [↑](#endnote-ref-11)
12. For more information about the IPPs, refer to OVIC’s *Guidelines to the Information Privacy Principles*, available at <https://ovic.vic.gov.au/privacy/guidelines-to-the-information-privacy-principles/>. [↑](#endnote-ref-12)
13. ‘Data collection standards – Aboriginal and Torres Strait Islander communities’, *Victorian Family Violence Data Collection Framework*, Department of Premier and Cabinet, State of Victoria, December 2019, available at <https://www.vic.gov.au/victorian-family-violence-data-collection-framework/data-collection-standards-aboriginal-and-torres>. [↑](#endnote-ref-13)
14. Australian Bureau of Statistics, ‘Key findings’, *4733.0* - *Information Paper: Review of the Indigenous Status Standard*, 2014, available at [www.abs.gov.au](http://www.abs.gov.au). [↑](#endnote-ref-14)
15. Australian Bureau of Statistics, *4726.0 - Information Paper: Perspectives on Aboriginal and Torres Strait Islander Identification in Selected Data Collection Contexts*, 2012, available at [www.abs.gov.au](http://www.abs.gov.au). [↑](#endnote-ref-15)
16. See OVIC’s *Guidelines to the Information Privacy Principles* for more information, available at <https://ovic.vic.gov.au/privacy/guidelines-to-the-information-privacy-principles/>. [↑](#endnote-ref-16)
17. For example, see the Australian Institute of Health and Welfare’s *National best practice guidelines for collecting Indigenous status in health data sets*, 2010, available at [www.aihw.gov.au](http://www.aihw.gov.au); see also The Australian National University and The Lowitja Institute’s report *Improving the identification of Aboriginal and Torres Strait Islander people in mainstream general practice*, 2010, available at [www.lowitja.org.au](http://www.lowitja.org.au). [↑](#endnote-ref-17)
18. For more information about consent, see the ‘Key Concepts’ chapter of the IPP Guidelines at <https://ovic.vic.gov.au/book/key-concepts/#Consent>. [↑](#endnote-ref-18)
19. Based on the National Aboriginal Community Controlled Health Organisation’s definition of ‘community control’, available at [www.naccho.org.au/definitions/communitycont.html](http://www.naccho.org.au/definitions/communitycont.html). [↑](#endnote-ref-19)
20. Page 59 of the *Victorian Aboriginal Affairs Framework 2018-2023* (**VAAF**), available at <https://www.aboriginalvictoria.vic.gov.au/victorian-aboriginal-affairs-framework-2018-2023>. The VAAF is the Victorian Government’s overarching framework for working with Aboriginal and Torres Strait Islander Victorians, organisations and the wider community to drive action and improve outcomes. [↑](#endnote-ref-20)
21. This was highlighted in the Australian Competition and Consumer Commission’s (**ACCC**) Digital Platforms Inquiry, which looked at the issue in the context of digital platforms. The ACCC’s *Digital Platforms Inquiry Final Report* (26 July 2019) is available at <https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report>. [↑](#endnote-ref-21)
22. For further guidance see the Department of the Prime Minister and Cabinet’s resource *Communicating with Aboriginal and Torres Strait Islander Audiences*, available at <https://www.pmc.gov.au/resource-centre/indigenous-affairs/communicating-aboriginal-and-torres-strait-islander-audiences>. [↑](#endnote-ref-22)
23. Australian Bureau of Statistics, *4726.0 - Information Paper: Perspectives on Aboriginal and Torres Strait Islander Identification in Selected Data Collection Contexts*, 2012, available at [www.abs.gov.au](http://www.abs.gov.au). [↑](#endnote-ref-23)
24. Page 5, *Strangers in their own land: Use of Aboriginal Interpreters by NT agencies*, Ombudsman NT, August 2018, available at <https://www.ombudsman.nt.gov.au/sites/default/files/downloads/interpreter_services_investigation_report.pdf>. [↑](#endnote-ref-24)
25. ‘Data collection standards – Aboriginal and Torres Strait Islander communities’, *Victorian Family Violence Data Collection Framework*, Department of Premier and Cabinet, State of Victoria, December 2019, available at <https://www.vic.gov.au/victorian-family-violence-data-collection-framework/data-collection-standards-aboriginal-and-torres>. [↑](#endnote-ref-25)
26. Australian Bureau of Statistics, *4726.0 - Information Paper: Perspectives on Aboriginal and Torres Strait Islander Identification in Selected Data Collection Contexts*, 2012, available at [www.abs.gov.au](http://www.abs.gov.au).

**Disclaimer:** The information in this document is general in nature and does not constitute legal advice. [↑](#endnote-ref-26)