Office of the Victorian Information Commissioner

IPP 1 – Collection

IPP 1 – Collection

On this page

1.1 Collection is a key part of the PDP Act and goes to the heart of information privacy protection. Collecting personal information attracts obligations under the IPPs, so it is crucial organisations get it right. If collected wrongly, organisations may be unable to use information in the way they envisaged.

1.2 The Macquarie Australian Dictionary defines 'collect' as 'to gather together' or 'accumulate'. The Victorian Civil and Administrative Tribunal (**VCAT**) has described collection as 'the manner in which an organisation *comes into possession* of personal information' (emphasis added).[1] An organisations has collected information when it has possession or control of that information, 'whether alone or jointly with other persons or bodies, irrespective of where the document is situated, whether in or outside Victoria'.[2]

1.3 When collecting information, organisations should first consider what information is necessary to carry out a particular function or activity, then consider whether the function or activity can be achieved without personal information, and last, whether the information can be anonymous or de-identified.

1.4 The best privacy safeguard is to not collect unnecessary personal information. If an organisation collects personal information it does not need, it will have to comply with all the other IPPs in relation to that information. The unnecessary collection may breach IPP 1.1, and later there may be a risk of breaching an IPP for information that did not need to be collected and held in the first place.

1.5 Organisations might avoid collecting information by not recording that information. When an employee hears or sights personal information without making a record, the organisation does not possess this information. There has been no collection. For example, it may not be necessary for an organisation's functions or activities to make a record of a person's identification document or Working with Children Check. In some circumstances, merely sighting this document may be sufficient for the organisation's functions. On the other hand, when an employee hears or sights personal information, and consequently makes a record of that personal information, the record is the possession of the organisation and collection has occurred.

1.6 The collection principles (IPPs 1 and 10) do not apply to information already collected by organisations before the *Information Privacy Act 2000* (Vic) (the first piece of Victorian privacy legislation), which was effective from 1 September 2001.[3] In contrast, the other IPPs do apply to information already held at that date.[4]

IPP 1.1: Necessary for one or more functions or activities

1.7 Under IPP 1.1, organisations must only collect personal information necessary for one or more of

[1] *Jurecek v Director of Transport Safety Victoria* (Human Rights) (Corrected) [2017] VCAT 1488 [39]; *Roberts v Anglicare Victoria* [2014] VCAT 1515 [24].

[2] PDP Act, s 4(1).

[3] *Information Privacy Act 2000* (Vic) s 15(1).

[4] Note: The Federal *Privacy Act 1988* differs in this regard. It imposes fewer obligations on private sector organisations when dealing with information already held prior to 21 December 2001 (when the private sector privacy provisions commenced) – see ss 16C and 16D of the *Privacy Act 1988* (Cth).

their functions or activities.

1.8 Therefore, organisations need to be clear about both the need for the personal information and the function or activity it relates to. Both elements are required.

Necessity

1.9 IPP 1 aims to ensure organisations only collect personal information necessary for their purposes and not collect personal information that is in excess of their requirements.

1.10 Organisations should take a practical approach to assessing necessity. The following questions may help in determining whether personal information is necessary for a function or activity.

- Does the organisation need the personal information to fulfil the function or activity effectively?
- Can the function or activity be achieved with anonymous information?

1.11 Some examples of when the collection of personal information is necessary include:

- when collecting information might be required by law, for example, when submitting an objection in relation to planning permits or other local government matters;
- in order to refer a complaint to the appropriate organisation or, in some cases, to successfully resolve a complaint;
- to confirm a person's identity to discuss information that includes personal information; and
- to collect information about an applicant's suitability for a role during a recruitment process.

1.12 Conversely, examples of unnecessary collection include:

- collecting information about a person's credit history before they have accepted a job offer;[5]
- collecting driver's licence information during a recruitment process for a role that does not require a person to hold a driver's licence to fulfil the functions of the role; and
- collecting personal information to complete a transaction or resolve a complaint, where collection is not required to complete it.

1.13 Collection of personal information should be for a specific purpose. The purpose must be closely tied to the organisation's functions or activities. The type and extent of personal information collected should be limited to the minimum amount necessary to achieve that purpose. For example, a contractor was engaged to conduct surveillance to use in assessing a compensation claim but the contractor surveilled the wrong person. The Privacy Commissioner concluded the information about the wrong target was not necessary for one or more of the organisation's functions.[6] To avoid excessive collection and retention of personal information, organisations should delete or destroy information not necessary to their functions or activities. This aligns with IPP 4.2.

1.14 In *Ng v Department of Education* [2005] VCAT 1054, the Department installed CCTV cameras in a computer classroom to minimise vandalism and monitor student use of the computers. VCAT considered whether CCTV monitoring of a classroom was necessary for the Department's function. While noting that it could be argued the education system in Victoria had operated for more than a century without the need for video surveillance, VCAT took a 'more relaxed meaning of necessity' and suggested the test:

[5] *Case Note 218236* [2011] NZPrivCmr 4.

[6] *Complainant X v Contracted Service Provider to a Department* [2005] VPrivCmr 6.

...is the collection in question here reasonably required or legally ancillary to the accomplishment of the Department's functions?[7]

1.15 VCAT found the use of CCTV for monitoring the computer rooms was reasonably required and supplementary to the Department's function in operating a school system. VCAT accepted the system was 'reasonably adapted to the attainment of the Department's functions in providing education in computer subjects' because the CCTV system could be turned on and off, rather than record constantly. There was no breach of IPP 1.1.[8]

1.16 In *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285 (***Jurecek***), Bell J upheld VCAT's approach in *Ng v Department of Education* [2005] VCAT 1054. See Case Study 1A below.

Case Study 1A: Organisation's collection of Facebook messages for a misconduct investigation found to be necessary[9]

The Complainant and a colleague exchanged messages over Facebook on a Facebook 'wall' and in private messages. Transport Safety Victoria (**TSV**) classified the Complainant's messages to the colleague as abusive and it carried out an investigation. TSV's investigation concluded the allegations against the Complainant of misconduct on social media were proven.

The Complainant complained TSV had breached IPP 1.1.

VCAT found TSV's collection of the Complainant's personal information was for a legitimate purpose - to investigate a misconduct investigation - so IPP 1.1 was not breached.

On appeal to the Victorian Supreme Court, Bell J upheld VCAT's finding that TSV had not breached IPP 1.1, stating 'there is nothing to suggest that the tribunal adopted a threshold of 'necessary' for the organisation's functions or activities that was too low'.

Bell J warned against an overly narrow reading of 'necessary':

'*The principle is intended to ensure that information collection by organisations is purposive and not an end in itself. While the intention is to confine the information collection to that which is necessary for the functions and activities of the organisation, it is not to restrain the reasonable performance of those functions and activities. To interpret 'necessary' narrowly would alter the proper balance between privacy protection and the conduct of public administration. It would not be consistent with the human right to privacy, which is neither absolute nor intended to interfere with the capacity of governmental organisations effectively to pursue their functions and activities. Therefore, in that principle, 'necessary' does not mean 'essential' or 'indispensable' but 'reasonably necessary' for the organisation's functions or activities, as correctly so decided by Macnamara DP in* Re Ng v Department of Education *… the concept of reasonable proportionality comes into that assessment.'*[10]

[7] *Ng v Department of Education* [2005] VCAT 1054 [84].

[8] *Ng v Department of Education* [2005] VCAT 1054 [85].

[9] *Jurecek v Director, Transport Safety Victoria* [2016] VSC 285 (***Jurecek***).

[10] *Jurecek* [103].

Collecting information at the time it is needed

1.17 Where appropriate, organisations should only collect personal information at the time it is necessary to fulfil the organisation's function or activity. For example, eligibility for a particular role may be subject to pre-employment screening such as a police check. However, an organisation may decide to collect the personal information required for the police check only once a preferred candidate has been selected, rather than collecting that information from all applicants for the position.

1.18 Another example may be where an organisation provides an online platform for individuals to register for or renew a licence. While collecting personal information such as payment details, which may be necessary to enable the organisation to process an application, the organisation may decide to collect that particular information at the time individuals apply for registration or renewal, rather than when they first sign up to use the platform.

Incidental collection

1.19 Sometimes organisations may collect incidental information about a person or third party that may not be strictly necessary to carry out their functions or activities. In *Complainant AE v Contracted Service Provider to a Statutory Authority* [2006] VPrivCmr 6 (***Complainant AE***), for example, surveillance was carried out on the Complainant's wife in relation to her claim for compensation. The surveillance also captured information about the Complainant, who argued his information was not necessary for the contracted service provider's function of assisting the statutory authority to assess the merits of his wife's claim. The Privacy Commissioner accepted that surveillance may, when carried out lawfully and appropriately, inevitably capture information about someone other than the person who is the intended subject of the surveillance. In some cases, information about the third party may be relevant information about the person under surveillance. In *Complainant AE*, information that a third party was driving the car shows the subject of the surveillance was not driving and this was relevant for her claim. The Privacy Commissioner suggested the following test to assist in determining when collecting incidental information about third parties during surveillance:

> *Information collected about the complainant is relevant information when a reasonable person would find sufficient connection between the subject of surveillance and the other party, the complainant.*[11]

1.20 A further discussion of the meaning of 'necessary' is contained in the Key Concepts chapter.

Function or activity

1.21 A public sector organisation's functions and activities are often based in law. A function or activity may be specifically listed in the organisation's enabling legislation or broadly expressed in statute and further refined in regulation, ministerial directive or other sources. An organisation should check these sources so it clearly understands its functions and activities. Over time, organisations may lose sight of the legal basis underpinning their functions or legislative reforms may change an organisation's functions or activities.

1.22 Organisations should be clear and specific about the function or activity for which the personal

[11] *Complainant AE v Contracted Service Provider to a Statutory Authority* [2006] VPrivCmr 6.

information is needed.

IPP 1.2: Lawful, fair, not unreasonably intrusive

1.23 IPP 1.2 requires information is collected only by lawful and fair means and not in an unreasonably intrusive way.

Lawful

1.24 Collection must be according to law and not contrary to law. This includes criminal and civil law, statute and common law.

1.25 Unlawful collections under the PDP Act include:

- collections of particular types of information that are prohibited by another law, such as restrictions against collecting particular information (for example, DNA profiles from bodily samples collected during roadside drug testing);12
- collections made in particular circumstances (for example, monitoring of private conversations or activities without consent or a warrant13 or the collector has trespassed to obtain the information); and
- collections made by an organisation that has improperly exercised its power to collect personal information or has exceeded its power.

Fair

1.26 IPP 1 prohibits 'unfair collection' of personal information Whether a person regards something as unfair is likely to be subjective and involve moral or ethical considerations. The High Court of Australia has suggested the concept of 'fairness' should be viewed in context and in accordance with community values:

> *The term 'unfairness' necessarily lacks precision; it involves an evaluation of circumstances… [F]airness is a concept broad enough to adapt to changing circumstances as well as evolving community values.*[14]

1.27 Information may be considered as unfairly obtained where it was collected by trickery, deception or under duress. Information may also have been unfairly obtained if it was collected in circumstances in which the individual would not have given up the information if proper procedures had been followed.[15]

1.28 Regarding the recording of a phone call without notice, the Australian Privacy Commissioner has said a determination as to whether collection is 'fair' requires consideration of:

> *all the circumstances, which may include issues going to the sensitivity or secrecy of the conversation, the reasonable expectations of participants, and the ease with which the*

---

[12] Analysing samples obtained during roadside drug testing to derive a DNA profile is prohibited by *Road Safety Act 1986* (Vic) s 58B.

[13] *Surveillance Devices Act 1999* (Vic) ss 6, 7.

[14] *R v Swaffield; Pavic v The Queen* [1998] HCA 1 [53] (Toohey, Gaudron and Gummow JJ), [131] (Kirby J).

[15] *R v Swaffield; Pavic v The Queen* [1998] HCA 1 [54], [71] (Toohey, Gaudron and Gummow JJ).

participants could be informed that a recording was being made.[16]

Examples of unfair collection

1.29 An organisation may not be collecting personal information fairly if, for example, it receives personal information from individuals that the organisation knows are under the mistaken belief they are required to provide the information. Individuals may be required by law to provide certain information, for example:

- to obtain or access a benefit or entitlement;
- to exercise a right or privilege;
- to obtain a licence for a profession; or
- to volunteer in child-related areas of work.

1.30 Legislation may set out the type of information that must be provided and, in some cases, may make it a criminal offence to provide false or misleading information. In these contexts, organisations that require individuals to provide more information than necessary should consider carefully whether they are collecting unfairly.

1.31 It may also be an unfair collection if an organisation misrepresents what will be done with the information once it is collected, for example, claiming the information will be treated securely and confidentially when it is intended that the information be passed on to others.

Case Study 1B: Failure to disclose use[17]

Before a meeting with one of its employees, Organisation A had promised complete confidentiality. The organisation later disclosed the employee's personal information (opinion) to others within the organisation. This led to the employee's dismissal. The employee had not been informed of how the information they provided would be used or disclosed.

The New Zealand Privacy Commissioner found a breach of Principle 3 of the *Privacy Act* 1993, which is similar to IPP 1. The New Zealand Privacy Commissioner stated an important element in the assessment of 'unfairness' is whether a complainant would have responded differently had he or she known how the information would be dealt with; in this case, the disclosure of the information.

1.32 Similarly, it may be unfair if an organisation collects information for one purpose, giving assurances or undertakings the information will not be used for any (or certain specified) purposes, and then make such a use or disclosure, especially where:

- individuals may not have provided their information if they had known what it would eventually be used for;
- less intrusive alternatives were available but were not considered; or

[16] '*LP' and The Westin Sydney* (Privacy) [2017] AICmr 53 [33].

[17] *Case Note 29987* [2003] NZPrivCmr 4.

- additional safeguards would have been sought regarding the secondary use.

Steps to ensure collection is fair

1.33 To avoid collecting personal information by unfair means, organisations must not misrepresent what personal information is compulsory to provide, and what is optional.

- When preparing forms, organisations should differentiate between different grounds of collection: information specifically required by law and information not required by law, but necessary for the organisation's functions or activities. Organisations should remember that information can be provided with consent but they should indicate to individuals when the provision of information is optional.
- When using electronic forms, organisations should design them so the individual is not forced to supply personal information that is optional.

1.34 Organisations should also ensure they do not misrepresent how an individual's personal information will be handled after it is collected.

- If an organisation is likely to use the individual's personal information for a secondary purpose or disclose it to a third party, the organisation should let the individual know (see Case Study 1B).
- If an organisation receives unsolicited personal information, it should consider providing notice of the collection, especially if that information may be subsequently disclosed and will have a significant impact upon the individual (see Case Study 1G).
- An individual should not receive mixed messages about how an organisation intends to use or disclose their personal information. Collection will be unfair if the organisation's collection notice sets out possible disclosures of the individual's personal information, while an employee assures the individual their information will be kept 'confidential'.

1.35 The simplest way for an organisation to avoid misrepresenting how it will use an individual's personal information is to ensure that it is complying with its notice obligations (see IPP 1.3).

Surveillance and fairness of collection

1.36 Organisations can use surveillance cameras and monitoring programs (for example, for staff email) to collect personal information of the public or staff, but they must use them in compliance with IPP 1.2.

1.37 Collecting information or monitoring individuals without notice and without their consent or knowledge, (for example, covert surveillance) is unfair in some circumstances. For example, in *'LP' and The Westin Sydney* (Privacy) [2017] AICmr 53, a hotel's recording of a guest's phone without their knowledge was found to be unfair.

1.38 There are some situations where the use of covert surveillance may be justified and not considered unfair, depending on how it is conducted, for example, where it is:

- expressly authorised under law by a decision maker required to take privacy interests into account, such as where a judge grants a covert warrant;
- carried out with prior notice that covert surveillance may be used for limited and specified purposes, such as to enable an employer to investigate suspected unlawful activity; or
- misconduct of a serious kind, or to allow an insurer to investigate a suspected fraudulent compensation claim.

1.39 In *Ng v Department of Education* [2005] VCAT 1054, VCAT found that there was no breach of IPP 1.2

as there was no apparent unlawfulness, and because Ng was aware that surveillance was underway and later implicitly consented to its use for assessing her performance in the classroom. VCAT did not appear to address the question of fairness at the time of collection. If it had, factors relevant to an assessment of fairness may have included:

- departmental guidelines (although not binding), which expressly forbade the use of CCTV use for monitoring individual work performance; and
- public notices and staff briefings which gave the impression that the CCTV would only be used to detect vandalism and graffiti and not for purposes related to teachers' employment.

1.40 Implied consent to a later use of the CCTV footage to assess performance does not affect whether the footage was collected fairly in the first place.

1.41 If an organisation is implementing surveillance, undertaking a Privacy Impact Assessment (**PIA**) is a good way to ensure the personal information it is capturing is done fairly. A PIA will help an organisation to:

- define and clearly articulate the purpose of the collection via surveillance. If an organisation is considering covert surveillance, identifying a legitimate need that justifies the use of this intrusive option is especially important;
- ensure the surveillance is limited in scope and duration;
- consider whether the privacy interests of any persons (including third parties) may be affected by the surveillance (see below); and
- put in place appropriate oversight and accountability mechanisms to deter and detect any misuse.

1.42 An organisation implementing surveillance should note and consider the likelihood of incidental collection of third parties' personal information.[18] Finally, organisations should make sure they meet their obligations under the *Charter of Human Rights and Responsibilities Act 2006* (Vic) (**Charter**).[19] The Charter requires organisations to consider the extent to which a collection practice affects other rights, if any. For example, although covert collection of personal information may be permitted in some cases, the line between what is permissible and what is not may be crossed where other rights are unduly infringed.

Not unreasonably intrusive

1.43 The phrase 'unreasonably intrusive way' in IPP 1.2 focuses on the method used to collect information. In contrast, the necessity test in IPP 1.1 concerns the type and amount of information collected.

1.44 In practice, there are often only fine distinctions between a collection that is unnecessary (IPP 1.1) and a collection done in an unreasonably intrusive way (IPP 1.2).

1.45 To illustrate this point, a collection may be unreasonably intrusive where excessive or unnecessarily intimate information is collected, or where the collection unreasonably interferes with a person's home life or their bodily integrity. Whether a collection is unreasonably intrusive will largely depend on the context and the need that is said to underpin the collection. Placing CCTV cameras in public and staff areas for safety and security reasons (with adequate signage) is not overly intrusive. However, installing a CCTV camera in a toilet area that captures highly sensitive images is likely to be

[18] See *Complainant AE* at paragraph [1.19] above.
[19] See especially s 38 of the Charter, which requires public authorities to act in a way that is compatible with human rights and to give proper consideration to relevant human rights when making decisions.

unreasonably intrusive, especially if the purpose for its location is unclear.[20]

1.46 Collecting information in 'ways not unreasonably intrusive' has to be assessed in all the circumstances. Asking an employer, neighbour or family member for information when the organisation could go directly to the person concerned may also be unreasonably intrusive, depending on the nature of the information and the circumstances of the relevant relationship. IPP 1.4 and IPP 1.5 are relevant where collection occurs via a third party.

1.47 What might be unreasonably intrusive in one context may not be in another. For example, requiring an iris scan from individuals who visit a highly secure facility may not be considered overly intrusive. However, the same practice may be unreasonably intrusive for a different facility, such as a library or public hospital.

1.48 It may also be unreasonably intrusive to collect information too soon from too many people. For example, asking all job applicants to undergo criminal record checks or medical examinations may be overly intrusive when it is reasonable to limit the request to a preferred candidate.

1.49 In whatever way the information is collected, organisations should be able to justify and explain the source of personal information and the method of collection.

IPP 1.3: Collection notices

1.50 IPP 1.3 requires organisations to take reasonable steps to make individuals aware of:

- the identity of the organisation and how to contact it;
- the fact they may access that information;
- the purposes for which the information is or was collected;
- the names (or types) of organisations or individuals to whom the information is usually disclosed;
- any law requiring the collection; and
- the main consequences (if any) if the person does not provide any or part of the information.

1.51 One way to make individuals aware of this information is to provide them with a collection notice. Notices provide individuals with the information they need to make decisions about their personal information. They also ensure individuals are aware of their rights and obligations in relation to giving and later accessing their information. As Bell J noted in *Jurecek*:

> *The main purpose of the notification requirement on IPP 1.3 is to promote governmental transparency and respect for the autonomy and dignity of individuals with respect to their personal information.*[21]

1.52 Please also refer to 'Reasonable steps' for giving notice under IPP 1.3 or IPP 1.5 and OVIC's other guidance materials, including Collection Notices Information Sheet.

1.53 It is not always necessary to include a collection notice in a letter requesting information. Sometimes, the text of the letter itself will contain the information required by IPP 1, in which case a

[20] *Case note 244873* [2013] NZ PrivCmr 5: Man objects to CCTV camera in the men's public toilets of a pub. As well as being 'unreasonably intrusive', collecting footage from a CCTV camera in a public toilet would also be unlawful, per *Surveillance Devices Act 1999* (Vic) s 7.

[21] *Jurecek* [120].

separate collection notice is not required.

When should a collection notice be provided?

1.54 Notice should be given before or at the time of collection. If that is not practicable, IPP 1.3 allows notice to be given as soon as practicable after the information is collected.

1.55 Providing prior notice generally gives individuals the opportunity to consider whether they will proceed with their interaction with government, knowing what information will be collected and how it will be used. For example, prior notice that successful job applicants will be required to undergo a criminal record check should be given at the time individuals apply to enable them to decide about whether to proceed with the application or not.

1.56 A collection notice should be provided to an individual each time the organisation collects personal information from them.[22] However, the notice does not need to include the same level of detail each time. Some matters, for example, the identity of the organisation, may be obvious from the context. Sometimes, the organisation will have already taken steps to notify an individual when the same or similar information was collected on a previous occasion.

1.57 When collecting personal information for different functions or activities, organisations need to provide more than one collection notice. This is because the purposes for collection, the type of information collected and the way the information is used and disclosed may differ with each activity. For example, information collected when receiving complaints from the general public will be different from information collected during a recruitment process, and it will be used in different ways.

1.58 Sometimes it may be impossible to give prior notice, for example, where emergency services are being delivered. In other cases, immediate notification might be unreasonable as it could jeopardise the integrity of an investigation, such as those involving disciplinary action. This was the case in *Jurecek* (see Case Study 1A above) where an employer collected employee's information for a misconduct investigation without informing the employee and from someone other than the individual. Bell J said:

> *'The concept of what is practicable necessarily involves an assessment that reasonably balances protection of privacy in relation to personal information with the purposes of collection. Considerations such as the nature of the information, what is at stake for the individual and the degree of the interference, on the other hand, and the public interest being served by the collection, on the other, come into play.*[23]

1.59 Bell J upheld VCAT's decision that IPPs 1.3 and 1.5 were not breached and found the decision was *'consistent with this concept of reasonable proportionality'*.[24] However, Bell J emphasised that such decisions about the timing of notification should be made on a case by case basis:

> *I am not suggesting, nor did the tribunal decide, that it will be considered practicable to delay notification in all such cases, for the issue will always turn on the facts and circumstances of the case and a reasonable balancing of the matters to which I have*

[22] See 'Layering collection notices' for more information.

[23] *Jurecek* [121].

[24] *Jurecek*.

referred.[25]

1.60 Where providing notice before or at the time of collection is not practicable, organisations should still take reasonable steps to give notice as soon as practicable after the collection. See Key Concepts for more information relating to 'practicable' and 'reasonable, reasonably'.

1.61 Law enforcement and certain other organisations, such as Information Sharing Entities (ISEs) and the Central Information Point (CIP), may be exempt from requirements in IPP 1.3 to IPP 1.5.[26] For more information, refer to 'When do the IPPs not apply?' in the Overview chapter.

Form of notice

1.62 Notice can be provided in different ways. It can be given to individuals, for example, via paper, online, perhaps in the form of online forms, or telephone scripts . Sometimes a simple explanation at the time of collection will be sufficient. Ideally, the notice should be easy to understand. This means it should not be a long, complicated online form in fine print. It should also not be so brief it does not communicate the necessary information listed above.[27]

1.63 The form of notice and how it is communicated to an individual is relevant when considering if reasonable steps have been taken. What is reasonable depends on the circumstances. This means sensitive personal information will require greater steps and perhaps a different form of notice. For example, a simple explanation of IPP 1.3 matters may not be enough.

Can notice be inferred or implied?

1.64 Notice is unlikely to be inferred. It will only be inferred in very limited circumstances, for example, because the specific individual has a high level of understanding of the organisation's functions. For example, in *Little v Melbourne City Council*, VCAT was satisfied Mr Little knew the organisation's functions and that the information was provided to raise a possible breach of the *Food Act*. As a result, the VCAT were 'satisfied' implicit notice was provided as to the purposes for which the information was collected.[28] See Case Study 1C for a similar example in NSW.

> **Case Study 1C: Notice inferred because the disclosure was a logical consequence of previous notice[29]**
>
> AIN complained her personal information had been disclosed by the Medical Council to the Australian Health Practitioner Regulation Agency (AHPRA), the national registration body created in 2010, without her being notified.
>
> The Medical Council argued, and the Tribunal accepted, the applicant had been told that information about her registration status, and the registration status of all other medical practitioners in NSW, would be transferred to AHPRA in 2010. The Tribunal accepted the

[25] *Jurecek*.

[26] PDP Act, ss 15, 15A and 15B.

[27] Privacy NSW, *A Guide to the Information Protection Principles*, 1999, pp 11-12.

[28] *Little v Melbourne City Council* (General) [2006] VCAT 2190 [22].

[29] *AIN v Medical Council of New South Wales* [2017] NSWCATAP 22.

applicant should have been aware that AHPRA would also be notified of conditions placed on her registration in 2011 as a 'logical consequence'.[30]

There was therefore no breach of IPP 3 for the Medical Council's failure to provide specific notice making AIN aware of to whom they would disclose that information (per IPP 1.3(d)).

On appeal, the Appeal Panel found the disclosure by the Medical Council to AHPRA was authorised under a different exemption.[31] Regardless, there was no breach because it could be inferred that AIN had received notice about the routine disclosures of conditions of registration to AHPRA.

1.65 Notice will rarely be inferred in situations involving a typical individual who does not have detailed knowledge of the organisation or its functions. Organisations should not assume ordinary members of the public will be familiar with their privacy rights under the PDP Act and aware of the information listed in IPP 1.3. If organisations fail to explicitly inform individuals of the information required under IPP 1.3 and assume notice will be inferred, it is unlikely they will meet the requirement of 'reasonable steps'. In *Jurecek*, Bell J makes the point that organisations should actively take reasonable steps to provide notice in accordance with IPP 1.3 and 1.5. Organisations cannot satisfy this obligation by assuming or 'speculating' on what the individual is aware of. Specifically:

> *'In relation to the collection of personal information about an individual, an organisation has a positive obligation under IPP 1.3 (and 1.5) to take reasonable steps to ensure [the individual is made aware of certain information]. It cannot discharge this obligation by speculating about whether the individual has awareness of the matters specified in paras (a)-(f). It cannot discharge the obligation by making a presumption or assumption about that subject.'*[32]

Multi-layered (or 'short') notices

1.66 Information required under IPP 1.3 can be provided in layers, from a full explanation to a brief refresher, as individuals become more familiar with how the organisation operates and what it does with their personal information. Brief privacy notices on forms or signs can be supplemented by longer notices made available online or in brochures. Organisations must make sure additional information in later 'layers' of a collection notice are easily accessible and current. Organisations should also remember collection notices must be specific for each individual instance of collection.[33]

1.67 When notice is given in layers, organisations should ensure individuals are able to easily locate and understand the required notification details of IPP 1.3. In some cases, it may be sufficient to post brief information on a sign. For example, where CCTV surveillance is conducted in an organisation, the sign might identify the organisation conducting the surveillance, briefly explain why there is

[30] *AIN v Medical Council of New South Wales* [2017] NSWCATAP 22 [57].

[31] *AIN v Medical Council of New South Wales* [2017] NSWCATAP 22 [90].

[32] *Jurecek* [128].

[33] See also the Office of New Zealand Privacy Commissioner, *Questions and Answers about Layered Privacy Notices*, available here.

surveillance and provide a website where individuals can find more complete details about IPP 1.3 matters. Video recording or photographing may also occur at events open to the public, for example, at a school fete or fundraising event. A short collection notice might explain that video recording or photographing may occur and provide contact information if members of the public want more information. This is an example of a layered collection notice.

The difference between privacy policies and collection notices

1.68 There is an important difference between an organisation's privacy policy and a collection notice. An organisation's privacy policy (which must be available to all who ask for it – IPP 5) broadly explains how the organisation manages personal information. It may not be detailed enough to explain the required matters in IPP 1.3 regarding that specific collection. Collection notices explain the information handling practices specific to the information collected from the individual and provide specific IPP 1.3 information.

1.69 For example, a local council's privacy policy will explain its information privacy practices and how it complies with the PDP Act according to its functions under the *Local Government Act 2004* (Vic). In contrast, a local council's collection notice should specifically explain what specific function the collection relates to, why the collection is necessary for that function and the other matters listed in IPP 1.3. A website privacy statement is one type of collection notice. A website privacy statement explains the information collected about the websites' users, and how the information will be used. It is not the same as the organisation's privacy policy because it only applies to information collection by access to the website.

The difference between consent and notice

1.70 Providing an individual with a collection notice does not equate to obtaining their consent for the collection, use or disclosure of their personal information. Information can be collected with consent, but consent is not always necessary. Nevertheless, notice requirements will generally apply.

1.71 Consent forms specify a reason for the collection, use or disclosure of personal information to get an individual's consent to a particular information handling practice. The individual may choose to give consent or not. In contrast, collection notices outline the information handling practices of organisations for a specific purpose and explain the matters of IPP 1.3 but do not provide the individual with the opportunity to consent to a specific information handling practice. For more information, see 'Notice versus consent' in Key Concepts.

IPP 1.3(a): Identifying the organisation

1.72 IPP 1.3(a) requires organisations to take reasonable steps to make the individual from whom personal information is being collected aware of 'the identity of the organisation and how to contact it'. This ensures individuals know who is collecting and handling their information and empowers them to contact the organisation, for example to get more information about the organisation or the collection.

IPP 1.3(b): Access to the information

1.73 Under IPP 1.3(b), organisations must take reasonable steps to make sure individuals are aware they are able to gain access to the personal information collected about them. This relates to an individual's rights under IPP 6 – Access and Correction.

1.74 Where the personal information is held by an organisation that is subject to the *Freedom of Information Act 1982* (Vic) (**FOI Act**), a request for access to that information should generally be made under the FOI Act. However, the FOI Act also allows organisations to provide access to information outside of the FOI Act.

1.75 IPP 6 will generally apply if an organisation is not subject to the FOI Act but *is* bound to the PDP Act, for example, a contracted service provider required to adhere to the IPPs under a provision in a State contract.

1.76 The fact an individual is able to access their personal information (irrespective of how a request is made) does not mean the individual will always get access to all of their information. There may be exemptions under the FOI Act or exceptions under IPP 6 that restrict access to all or parts of the information. Organisations should keep this in mind in case of queries from the public.

IPP 1.3(c): Purposes of collection

1.77 IPP 1.3(c) requires organisations to inform individuals of the purposes for which information is being collected. Organisations should aim to list all known purposes for which they are collecting that personal information from individuals, to make sure the organisation can use the information as it intends.

1.78 The primary purpose needs to be clearly stated and generally must be more specific than a reference to some broad power, for example, 'administering revenue laws', 'licensing', 'oversight of planning' or 'peace and good order'. A narrow primary purpose does not prevent the organisation from using or disclosing the information appropriately for related secondary purposes (under IPP 2.1(a)). When there are several purposes in statute which governs the organisation, each of these may be regarded as a primary purpose for IPP 1.

1.79 Organisations should notify individuals of any secondary purposes if they are known in advance. Individuals are more likely to accept secondary purposes of their personal information when organisations are upfront about how they will use the information they are collecting. See the discussions in Key Concepts of 'purpose' and 'function creep'.

IPP 1.3(d): Usual recipients of the information

1.80 IPP 1.3(d) requires organisations to ensure individuals are aware of who the information is usually disclosed to. This is to ensure individuals are informed of where their personal information is likely to go.

1.81 Organisations may list the individuals or organisations by name or by type. For example, a notice might state information is usually disclosed to the 'State Revenue Office and Australian Taxation Office' or the 'Victorian Electoral Commission and Australian Electoral Commission', or the notice might say information is disclosed to 'state and federal taxation authorities' or 'state and federal

electoral commissions'.

1.82 The notice should also mention when the information is usually shared for specific purposes. For example, the notice might say information is usually disclosed to 'state and federal electoral commissions for the purpose of updating the joint electoral roll'.

1.83 When an organisation collects personal information with the intention of publishing or disseminating it, for example, online, the organisation should clearly communicate this intention at the time of collection.

Case Study 1D: Online publication of submission to council without prior notice[34]

A local council called for submissions relating to an amendment to a local law. Any person affected by the amendment was able to make a submission under s 223 of the *Local Government Act 1984* (Vic). The complainant submitted a letter regarding the local law to the council, which contained the complainant's name and address, and general comments regarding his neighbours who were also identifiable.

The local council held a Special Council Meeting at which it considered the submissions relating to the local law, including the complainant's letter. After the meeting, the council published the minutes of the meeting on its website, attaching all of the submissions to the minutes, including the complainant's. This meant the complainant's name and address were now publicly available and could be found by using a search engine.

The complainant complained to the local council, requesting his letter be removed from the minutes. The local council responded stating the minutes of the meeting were required to be made available to the public. In addition, the council stated that s 223 submissions were required to be made available for public inspection in accordance with the procedures specified in the Act. The local council felt it had acted appropriately and would not remove the complainant's letter from its website.

The Privacy Commissioner considered the notice given to the complainant at the time of collection. In particular, the requirements of IPP 1.3 to take reasonable steps to ensure an individual knows the purpose for which information is collected and to whom and how it is usually disclosed, particularly if information is intended to be disclosed to the world at large (for example online). While the notice given to the complainant stated submissions would be considered at a Special Council Meeting, the notice did not state they would also be published on the council's website.

The complaint was resolved at conciliation. The council agreed to amend its collection statement and privacy policy.

1.84 Where lawful and practicable, organisations should consider allowing individuals to restrict the

[34] *Complainant AT v Local Council* [2011] VPrivCmr 2. See also *Complainant AL v Local Council* [2009] VPrivCmr 1.

publication of their personal information, for example, where the individual is concerned disclosure may pose a risk to their personal safety. Some laws expressly offer this option to restrict publication or disclosure of personal information.[35] In other cases, an organisation may exercise its discretion.

Case Study 1E: Online publication of delicate information without prior notice[36]

The complainant held a licence in relation to a sensitive trade activity under a statutory scheme. When she registered with the statutory entity who administered the scheme, she was unaware her name would be included on the register that subsequently became available on the internet. Google searches led to results associating her name with another related and more sensitive trade activity, also regulated by the statutory entity. She felt humiliated about being wrongly identified with the more sensitive trade and was concerned about the risk of harm that may result from being identified and then located.

The statutory entity removed the register from the internet and later worked with Google and an internet archive to remove any cached copies of the information that was still accessible to searchers.

IPP 1.3(e): Compulsory collection

1.85 Where an organisation has the power to collect information compulsorily, that power should be made clear to the individual. The collection notice should specify which law authorises the mandatory collection. This makes the organisation's legal authority transparent and allows individuals to check the scope of that authority. It also encourages the organisation itself to check the collection is lawful and not excessive or intrusive (IPP 1.2).

1.86 If the information is required under law for one purpose but not for other purposes, this should be stated in the notice.

Optional information

1.87 Where an individual has the option to provide certain details voluntarily (for example, email address, phone number, age or name), this should be made clear. Such information may still be considered necessary to an organisation because it assists the organisation to carry out its functions or activities effectively and efficiently, however there may be occasions where the individual does not wish to participate in all of the organisation's activities and so may prefer to withhold certain information.

1.88 Even where individuals have the option to provide personal information voluntarily, organisations still need to ensure this information is necessary to their functions or activities and is collected fairly and not unreasonably intrusively. An individual providing their information voluntarily does not mean IPPs 1.1 and 1.2 no longer apply.

[35] See, for example, the silent elector provisions in the *Electoral Act 2002* (Vic) s 31.

[36] *Complainant E v Statutory Entity* [2003] VPrivCmr 5.

IPP 1.3(f): Consequences for individuals who do not provide their information

1.89 IPP 1.3(f) requires organisations to give notice of the consequences (if any) for the individual if they choose not to provide all or part of the personal information requested. For example, organisations may not be able to provide a full range of services if certain information is not provided.

IPP 1.4: Direct collection

1.90 IPP 1.4 requires organisations to obtain information about an individual only from that individual, where it is lawful and practicable to do so. As Bell J noted in *Jurecek*, '*IPP 1.4 operates objectively … to collect such information other than from the individual must be objectively 'reasonable and practicable' whether the organisation thinks so or not*'.[37]

1.91 Collecting directly from individuals gives them control over what is collected, by whom and for what purposes. It provides individuals with an opportunity to refuse to participate in the collection, or to provide their information on conditions or with reassurances about how it is to be used. Direct collection also makes it more likely the information collected will be relevant, accurate, complete and up to date (as required by IPP 3 (Data Quality). This is because firsthand information is less likely to suffer from the data quality problems often associated with second-hand information.

1.92 Nonetheless, there will be many circumstances where it would not be practicable to collect information directly from the individual. This may occur in the context of an investigation, or where an individual discloses information about other family members when applying for financial assistance or welfare benefits.

1.93 As a result of indirect collection, organisations may end up collecting a considerable amount of information about individuals without those individuals' knowledge. In many circumstances, particularly where the information could be used to affect their interests, these individuals may want to know that their information has been collected, find out what is known about them and be informed about where their information might end up. That is what IPP 1.5 requires.

Case Study 1F: Indirect collection and its impact upon a Complainant

An organisation wrote a legal assessment about an individual based on information the organisation had collected from a third party.

The individual alleged that because the organisation had collected the information indirectly, the individual did not have the opportunity to provide important supplementary information.

In response to a complaint to the organisation and OVIC, the organisation agreed to change its practices. The organisation now attempts direct collection first, and resorts to indirect collection only when direct collection is unsuccessful.

[37] *Jurecek* [150].

IPP 1.5: Notice of indirect collection

1.94 There will be times when an organisation collects information about an individual from another individual, organisation or source. IPP 1.5 requires organisations to take reasonable steps to make an individual aware of the matters in IPP 1.3 if they collect personal information about that individual from someone else, unless doing so would pose a serious risk to the life or health of any individual, for example, in family violence matters.

1.95 Similar to IPP 1.3, IPP 1.5 promotes transparency about who is collecting individuals' information and why. It also ensures individuals are aware of their rights of access and obligations in relation to the collection of their personal information.

'Reasonable steps' for giving notice under IPP 1.3 or IPP 1.5

1.96 Determining whether it is practicable to give an individual notice as required by IPP 1.3 (including where the information is unsolicited), or what reasonable steps should be taken under IPP 1.5 to make identifiable individuals aware of the matters in IPP 1.3, will depend on the circumstances. Organisations may consider a number of factors, including:

- whether the organisation intends to respond to the sender (or third party) in any event, for example, to acknowledge receipt of the letter;
- whether notice is likely to have already been received by the sender, for example in previous correspondence or where the sender appears to be responding to information the organisation had made available and that information already contains a notice statement;
- the number of people likely to have access to the information;
- whether and how the organisation is likely to use or disclose the information;
- the likely effect on the individual, in particular any adverse effect of any future use or disclosure of the information;
- the type of personal information[38] (for example, sensitive or delicate information may require greater steps);
- the effect on the privacy of any other individual; and
- the ability of the organisation to contact the individual concerned.

1.97 Organisations may decide, in light of the factors above, it is not necessary or practicable to give (further) notice, or it is not reasonable to take steps to give notice. For example, an organisation may decide it is not reasonable to give notice if it would need to collect additional information about the individual to contact them.

1.98 If an organisation proposes to use, disclose, transfer, give access to, correct, update or complete unsolicited personal information, it should make further efforts to give notice under IPP 1.3 or 1.5.

1.99 For more information on the concept of 'Reasonable', see Key Concepts.

IPP 1 in practice

1.100 IPP 1 requires an organisation not to collect personal information unless the information is necessary for one or more of its functions or activities. Additionally, IPP 1 requires that an organisation must

[38] *HW v Office of the Director of Public Prosecutions (No 2)* [2004] NSWADT 73 [36].

collect personal information in a lawful and fair manner, and not in an unreasonably intrusive way. When an organisation collects personal information, either directly or indirectly, it must take reasonable steps to ensure the individual is aware of the matters in IPP 1.3. Collection directly from the individual is preferred. This part of the chapter discusses IPP 1 as it applies to a range of different situations.

Unsolicited personal information

1.101 Victorian public sector organisations do not always request, seek or actively gather the personal information they hold. The provision of information may be completely unsolicited. For example, an organisation may have a general function to receive information that is not specifically solicited. A regulator may receive enquiries or complaints, or ministers may receive letters from members of the community that include unsolicited personal information.

1.102 Sometimes, an organisation may ask for particular types of personal information but be provided with more information than was requested. For example, unsolicited personal information may contain the personal information of the provider and third parties. Unsolicited personal information may often be unnecessary for the organisation's functions and activities.

1.103 The IPPs apply to personal information, whether it is solicited or not. The PDP Act does not expressly exclude unsolicited information from the meaning of collection (as the NSW and New Zealand privacy laws do),[39] or limit the application of IPP 1 to solicited information (as the Commonwealth and Tasmanian privacy laws do).[40]

1.104 Examples of unsolicited personal information may include:

- a letter sent to an organisation in error;
- a misdirected email intended for another recipient;
- an email enquiry about a service provided by an organisation;
- a resume submitted to an organisation not in response to an advertised job vacancy;
- a petition containing names and contact details of residents sent to a council; or
- information provided during a phone call the organisation receives and records, that is additional to what is necessary for the organisation's needs.

1.105 Where an organisation receives unsolicited personal information unnecessary for its functions or activities, the organisation should consider its recordkeeping obligations under the *Public Records Act 1973* (Vic) (**Public Records Act**). The Public Records Act requires records be handled and disposed of in prescribed ways for recordkeeping purposes.[41] If the Public Records Act does not require organisations to keep the unsolicited personal information, organisations should dispose of it, either by returning the information or by destroying it. Organisations may be able to dispose of such information in accordance with the Public Records Act, for example, under Normal Administrative Practice.[42]

---

[39] *Privacy and Personal Information Protection Act 1998* (NSW) s 4(5); *Privacy Act 1993* (NZ) s 2.

[40] Australian Privacy Principle 4, Schedule 1, Part 2, *Privacy Act 1988* (Cth); *Personal Information Protection Act 2004* (Tas) s 11. Also note that, under the New Zealand legislation, organisations are not required to give notice where notice had been given on a previous occasion or where the lack of notice would not prejudice the interests of the individual concerned: *Privacy Act 1993* (NZ) s 6 (Principle 3(4)).

[41] *Public Records Act 1973* (Vic), s 12 and related Standards issued by Public Record Office Victoria.

[42] For more information on Normal Administrative Practice see https://prov.vic.gov.au/ or contact Public Record Office Victoria.

1.106 Disposal of unsolicited personal information is also consistent with IPP 4.2 which requires organisations to take reasonable steps to destroy (or permanently de-identify) personal information when it is no longer needed. However, if the Public Records Act requires organisations to retain unnecessary unsolicited personal information, the Public Records Act will prevail over the PDP Act to the extent of the inconsistency.[43]

1.107 The receipt of unsolicited information may trigger the notice requirements in IPPs 1.3 and 1.5. These provisions require reasonable steps to be taken to give notice at the time of, or as soon as practicable after, personal information is collected.

1.108 In some cases, it may not be reasonable to give notice. In *Little v Melbourne City Council* (General) [2006] VCAT 2190, for example, the Tribunal found the Council was not required to give notice under IPP 1.3 relating to an unsolicited letter sent by the Complainant to the Council prior to or at the time of collection. This was because it would be impossible to give notice at that point in time, as the information was unsolicited. Whether an organisation will need to take steps to give notice will depend on what is reasonable in the circumstances.

1.109 In other cases, it may be reasonable to provide notice of collection of unsolicited personal information:

Case Study 1G: Failure to take reasonable steps under IPP 1.3 when unsolicited personal information collected

The Complainant contacted Organisation A to report a workplace issue. During a call to set up an appointment, the Complainant disclosed that they were a survivor of a sexual assault that had occurred decades earlier. While the Complainant made it clear to Organisation A they did not want or need any assistance in relation to the sexual assault, Organisation A was aware at the time of receiving this information that it would need to disclose the information to other parties.

Organisation A made further contact with the Complainant several times in relation to their workplace issue, however, ultimately the Complainant decided not to use Organisation A's services. Over a year later, the Complainant was contacted by Organisation B about the sexual assault. The Complainant discovered that Organisation A had disclosed their personal information (regarding the sexual assault) to Organisation B.

In these circumstances, it would have been reasonable to provide notice under IPP 1.3 particularly given the nature of the information, the impact upon the individual when the information was further disclosed, and the fact Organisation A was aware at the time of collection it would be disclosing the information to Organisation B. Organisation A also had several opportunities to inform the Complainant it had or would disclose the information to Organisation B.

While the Complainant made it clear to Organisation A they did not want or need any assistance in relation to the sexual assault, Organisation A was aware at the time of receiving this information that it would need to disclose the information to another agency

[43] PDP Act s 6.

to meet certain statutory reporting obligations.

Understanding the risks of collection by completing a privacy impact assessment

1.110 When organisations undertake new collection of personal information, completing a privacy impact assessment (**PIA**) can assist in identifying whether the personal information being collected is necessary, as required by IPP 1. A PIA assesses the privacy impacts and risks of collecting certain information, allowing organisations to better judge if collecting that personal information is necessary for their purpose or merely supplementary. See OVIC's PIA guidance.

1.111 When organisations collect personal information, it is best practice to try to anticipate secondary uses of that information. A PIA can help do this. When an organisation has anticipated secondary uses, the collection notice to the individual can include these as purposes for which the information is being collected, as required by IPP 1.3(c).

1.112 A PIA also encourages organisations to think about how the personal information could impact the individual, as well as whether the collection of that personal information aligns with community expectations about what is or is not a reasonable collection. A collection permitted under law does not necessarily mean the public will consider it to be an acceptable collection. A collection that aligns with community expectations can foster public trust and acceptance and build confidence in the organisation.

Collecting information that could become identifiable

1.113 In some cases, organisations may collect information that, on the face of it, does not relate to an identifiable individual or appear to be information from which an individual's identity can be reasonably ascertained, such as data about an individual's mobile device or location data. However, while the information itself does not identify any individual, it may be combined with other information or databases, or if collected over an extended period of time uncover patterns and trends, to reveal an individual's identity. If that occurs, the information is personal information and all the requirements and protections of the IPPs will attach to it.

1.114 The test to determine if information is personal information for the purposes of the PDP Act is the 'reasonably ascertainable' test. Organisations should consider if an individual's identity can reasonably be ascertained from the data, perhaps due to aggregation or patterns. Only information from which an individual's identity can reasonably be ascertained is personal information under the PDP Act. To apply this test, organisations should look to the discussion of 'Reasonable' in the Key Concepts, and consider technological realities. For example, combining the unique machine address for computers, such as IP addresses, with other data sets or extraneous information would likely meet the 'reasonably ascertainable test'.

1.115 Whether non-identifiable information risks becoming personal information depends on the circumstances. Where organisations do not or cannot have full control or knowledge of the different contexts in which the non-identifiable information will be used, the risk of the information becoming identifiable is likely to be greater. Similarly, the risk increases where unit-record level information is concerned, compared to aggregate data.

1.116 This risk was illustrated by the release of data about public transport trips by Public Transport

Victoria in 2018.[44] In investigating the release, the Commissioner found that people's identities could be reasonably ascertained by linking the data with other information. As such, it was personal information and subject to the IPPs.

1.117 Where there is uncertainty about whether information is 'personal information' at the time of collection, organisations are encouraged to err on the side of caution and assume that the information is personally identifiable. This would include collecting the information in accordance with IPP 1.

Automated collection

1.118 The PDP Act applies to personal information, whether collected by manual or by automated means. Automated collection of personal information may occur through the use of technologies such as anti-virus software,[45] video surveillance,[46] use of cookies,[47] and website analytics. Many of these activities are commonplace and likely to be reasonably expected by members of the community. For example, website users should reasonably expect that certain limited information about their browsing habits will be collected when they visit websites. However, this collection of information may still raise privacy issues that organisations should consider. The most common issues are outlined in this section.

1.119 Web analytics monitor the behaviour of website users and collect user data, such as IP addresses. Organisations should seek to provide notice about the collection of this information, for example, by referring to it in their website collection notice. They should also apply the collection minimisation principle and collect only the minimum information necessary for their functions and activities.

1.120 Automated collection and monitoring may result in organisations collecting vast amounts of data, some of which may be sensitive information (as defined in the PDP Act) and some of which may not relate to the organisation's functions or activities (for example, personal emails or documents).

1.121 Even when organisations automatically collect information from individuals, organisations must take reasonable steps to make the individual aware of what information is being collected.

> **Case Study 1H: Necessary to clearly inform individuals of different forms of automatic collection (New Zealand)**[48]
>
> An employer included a notice of automatic collection of information from work computers in its employment agreement and employee manual. However, the notice did not explicitly state the monitoring software collected key stroke information.
>
> The NZ Privacy Commissioner considered that explicit notice of key stroke logging was required.
>
> This was in light of the ability of this monitoring technique to learn delicate and sensitive information, for example, passwords. The NZ Privacy Commissioner found the organisation

[44] OVIC, 'Disclosure of myki travel information' (Report, 15 August 2019) [52].

[45] *Complainant W v Public Library* [2005] VPrivCmr 5.

[46] *Ng v Department of Education* [2005] VCAT 1054.

[47] *Complainant L v Tertiary Institution* [2004] VPrivCmr 6.

[48] *Case note 229558* [2012] NZ PrivCmr.

had not provided sufficient notice regarding this collection. This constituted a breach of the NZ collection requirements.

The NZ Privacy Commissioner also found this collection was unnecessary and disproportionate to the employer's needs and breached Principle 1, that collection must be connected to and necessary for an organisation's functions and needs.

1.122 When automated systems are being set up or operated, organisations should do a PIA or take other steps to ensure:

- the collection or monitoring fulfils a legitimate purpose that relates to the organisation's functions or activities;
- the personal information collected is kept to the minimum necessary to achieve that purpose and proportionate to the apprehended 'risk';
- the least intrusive method of collection or monitoring is adopted; and,
- the information collection and handling practices are transparent and documented, with proper notice given to individuals about the matters required in IPP 1.3.

Case Study 1I: Constant automatic collection of audio in workplace unnecessary and intrusive (New Zealand)[49]

An employee was aware of surveillance devices in his workplace. However, he was not aware the camera had an audio recording capacity. The employee complained that personal phone calls had been recorded without his knowing.

The employer suggested the employees were not (or should not be) acting in a personal capacity during work hours, so the information recorded (collected) was not personal. However, the phone conversations did constitute personal information because personal information is any information about an identifiable person (see 'personal information' in Key Concepts).

The employer suggested collection was necessary to prevent and manage incidents. However, the NZ Privacy Commissioner found the collection was unnecessary because there were few incidents in the workplace and disproportionate and unreasonable because constant audio recording was intrusive in the circumstances.

1.123 Organisations may have other legal obligations relevant to their use of automated technologies for monitoring and collecting personal information, including laws relating to:

- the monitoring of telecommunications and stored communications (such as email) under the

[49] *Case note 289943* [2018] NZPrivCmr 5.

Telecommunications (Interception) Act 1978 (Cth);

- the monitoring or recording in relation to the input or output of information from a computer under the Surveillance Devices Act 1999 (Vic);
- the use of video and audio surveillance, and tracking technologies under the Surveillance Devices Act 1999 (Vic); and
- the unauthorised access to, and impairment or modification of, computer functions and electronic communications (and other related computer offences) under the *Crimes Act 1958* (Vic).

IPP 1 and the other IPPs

1.124 IPP 1 interacts with a number of the other IPPs, namely IPP 2 Use and Disclosure, IPP 8 (Anonymity) and IPP 10 (Sensitive Information).

1.125 Under IPP 1, an organisation must only collect personal information if it is necessary for the organisation's functions or activities. This requires organisations to have a clear purpose for collecting personal information. Identifying the purpose of collection is essential as it will help determine authorised uses and disclosures (IPP 2). Generally, under IPP 2 personal information can only be used and disclosed for the purpose for which it was collected. See IPP 2 of the Guidelines for more information about use and disclosure.

1.126 When collecting personal information, organisations should consider whether identifying information is needed for the organisation to fulfil its function or activity. If it is lawful and practicable, organisations must give individuals the option of being anonymous when entering into a transaction – this is the purpose of IPP 8 (Anonymity).

1.127 IPP 1 should be considered together with IPP 10 (Sensitive Information), which relates to the collection of sensitive information. IPP 10 aims to provide additional protections to IPP 1 by limiting the circumstances in which organisations can collect sensitive information.[50] See the discussion in IPP 10 of the Guidelines for more information.

> Please send any queries or suggested changes to privacy@ovic.vic.gov.au. We will respond to privacy enquiries and consider your suggestions when we next update the Guidelines to the Information Privacy Principles.

[50] Explanatory Memorandum, Privacy and Data Protection Bill (Vic) 36.

Version control table

Version	Description	Date published
IPP 1 – Collection 2019.B	Edits following consultation.	14 November 2019
IPP 1: Collection 2019.A	Consultation draft.	16 May 2019
IPP 1: Collection (2011)	2011 pdf version.	2011