

Australian Privacy Law Handbook

Douglas-Stewart

PRESIDIAN

LEGAL PUBLICATIONS

SAMPLE ONLY



Pages 2-1,011 are not part of this book preview.

Annotated National Privacy Principles

[3.10] NPP 1 – Collection

Publications, guidelines and related materials

- OPC, *Guidelines to the NPPs* (2001) at pp 27-34
- OPC, *Information Sheet 17 – 2003 Privacy and Personal Information that is Publicly Available*
- OPC, *Information Sheet 8 – 2001 Contractors*

"Collect"

[3.20] Collection includes the acquisition of personal information from any source, by any means and in any form (*NPPG* p 22). This is so irrespective of whether the information was sought by the organisation: *M v Financial Institution* [2009] PrivCmrA 16.

Collections to which Act applies

[3.25] When personal information is being collected by an organisation, the Privacy Act only applies, subject to limited exceptions, to that collection if the information is being collected for inclusion in a “record” or a “generally available publication” within the meaning of the Act (s 16B(1)). Accordingly, if an organisation collects personal information for inclusion in a document that falls outside the meaning of either of these terms, the collection is not covered by NPP 1.

The fact that the Act applies to a collection of information that is to be included in a generally available publication is not inconsistent with the fact that such information will not be subject to the Act once it is included in such a publication (see [14.255]). It simply means that the information will be regulated by the Act during the period from when it is collected to when it is included in the generally available publication – see [14.255].

NPP 1 only applies to collections after 21 December 2001 (see [14.275]).

Unsolicited information

[3.30] Unsolicited information is generally information that an organisation obtains but did not seek to collect or prompt anyone to provide (for commentary on what constitutes a “solicited” collection, see [5.85] under the Annotated IPPs).

The application of NPP 1 to unsolicited personal information is unclear. The Privacy Commissioner has found that passive receipt of information will not always amount to “collecting” information: *Seven Network v Media Entertainment and Arts Alliance* [2004] FCA 637 at [45]. However, in *E v Private School* [2010] PrivCmrA 6, the Commissioner held that the NPPs apply to both solicited and unsolicited information. Section 16B(1) provides that the NPPs apply to the collection of personal information “only if the information is collected for inclusion in a record or a generally available publication” although it is uncertain how this applies in the context of unsolicited information that, for example, is sent to the organisation in a document that falls within the meaning of a “record”, such as a letter. Arguably, if an organisation has been sent unsolicited personal information but does not intend to keep it, the collection may not need to comply with NPP 1, although it would be preferable to assume that NPP 1 does apply. It is clear, however, that if an organisation keeps unsolicited information, or any other personal information that it did not intend to acquire but which has come into its possession, it must be handled in accordance with the Act (s 16B(2)) (see also: *NPPG* at p 22; *M v Financial Institution* [2009] PrivCmrA 16).

In *Seven Network v Media Entertainment and Arts Alliance* [2004] FCA 637, the respondent failed to lead acceptable evidence on how it obtained information in order to protect the identity of the source of the information. The court held (at [45]) that this led to an inference that any such evidence would not assist its case and that some active step was taken to obtain the information.

[3.38]

1.1 An organisation must not collect personal information unless the information is necessary for one or more of its functions or activities.

Overview and operation

[3.39] NPP 1.1 means that an organisation cannot collect information for which it has no current or planned future need. One way in which organisations often breach this principle is by requesting irrelevant information from customers on application forms, either because the question directly requests irrelevant information or, more commonly, because the question is drafted too broadly.

However, where personal information is collected in the context of providing a particular good or service, NPP 1.1 does not mean that the organisation cannot request information for other purposes at the same time. For example, a credit union loan application form may request information that will be used by the credit union for marketing purposes. Whilst the marketing information will not be needed for loan assessment purposes, the information is “necessary” for marketing activities it conducts and its collection will therefore generally be permitted under NPP 1.1.

“Necessary”

[3.40] Generally, personal information will be deemed “necessary” if an organisation cannot effectively pursue a legitimate function or activity without collecting it. Information will not be deemed necessary if it is collected merely for the possibility that it may become necessary for one of the organisation’s future functions or activities that have not yet been planned or for which it is not yet certain what types of information will be required (*NPPG* p 27).

The Privacy Commissioner provided further guidance on the meaning of “necessary” in *Complaint Determination No. 4 of 2004*. The Commissioner stated (at [48]-[49]):

...I note...the comments of Gummow J in *General Newspapers Pty Limited and Others v Telstra Corporation* (1993) 117 ALR 629 (considering the meaning of 'necessary' within section 236(1) of the *Telecommunications Act 1991*):

The term 'necessary' will take its colour from its context; in ordinary usage it may mean, at one end of the scale, 'indispensable' and at the other end 'useful' or 'expedient': *Re an Inquiry under the Company Securities (Insider Dealing) Act 1985* [1988] AC 660 at 704.

I find that the use of the word 'necessary'... falls between the two ends of the scale identified by Gummow J. In my view it does not require that the information be indispensable to an organisation, in that, without such information, it would be impossible to carry on its business. It will not, however, be sufficient to show that the information is merely 'useful' or 'expedient'. Rather, determining whether or not the collection of personal information is 'necessary' requires consideration of whether or not it is clearly appropriate and relevant to the functions or activities of the organisation. In my view, information that is only of marginal relevance to the functions or activities of an organisation is more likely to be considered unnecessary for the purposes of NPP 1.1. It will also be relevant to consider whether or not the functions or activities of the organisation can be reasonably performed in a manner which does not require the collection of personal information. It may also be relevant to consider whether the information is of a sensitive nature such that it may be considered to be more invasive of a person's privacy.

NPP 1.1 does not limit the types of activities in which an organisation may engage; rather, it only limits the types of information an organisation may collect in view of the activities in which it chooses to engage. In *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005), the Commissioner stated (at p 83):

NPP 1.1 limits the collection of personal information by an organisation to that necessary for its 'functions or activities'. The organisation itself, however, determines what its functions and activities are

...

Accordingly, whether information is “necessary” is determined based on the activities in which an organisation engages rather than any assessment of the merits of an activity in which the organisation

engages (ie whether the organisation “should” be conducting a particular activity). To adopt the latter test would be to introduce a concept akin to the doctrine of ultra-vires whereby the types of legal activities in which an organisation may engage are limited by reference to, for example, some over-arching “purpose” of the organisation.

Cases

Collection forms

[3.45] *D v Banking Institution* [2006] PrivCmrA 4: A bank required marital status information from C who wished to open a bank account. C objected on the grounds that it was unnecessary for the purposes of opening the account, but the bank advised that its system did not allow certain accounts to be opened without entering information in the ‘marital status’ field. The bank stated that modifications to its system to enable individuals to open accounts without disclosing marital status would take some time and proposed that, to open an account for C, it would enter “single” in the data field and include a note stating that the entry may not reflect actual marital status. The bank agreed that the collection of marital status information was not necessary as it had no bearing on C’s eligibility to open the account. *Outcome:* The bank agreed that it would change its computer system so that an individual could refuse to provide marital status information. The banking institution committed to providing the Commissioner with quarterly reports on the progress of its implementation program. The bank also resolved to raise the issue of marital status collection with its industry body as it appeared to be an industry-wide practice.

***OPC v Employment Services Company* [2005] PrivCmrA 13:** The respondent, an employment services company, had been requiring applicants to provide a large amount of personal information, including tax file numbers and credit card details. *Outcome:* Requiring applicants to provide credit card details on application forms was an unnecessary collection of information and breached NPP 1.1 as an individual who had obtained a placement did not have to pay by credit card. The respondent removed the requests on forms for credit card details.

Consent forms

[3.47] *N v Private Insurer* [2003] PrivCmrA 12: An insurer’s privacy consent forms were drafted broadly to enable it to obtain any information from C’s health service providers, without limiting the consent to information that was relevant to a claim. The consent form provided “I authorise any medical attendant consulted by me or any hospital attended by me, to divulge to [the insurer] or any legal tribunal, any health or other information acquired with regard to myself.” Further, the form did not limit the period for which the consent was valid. The statement was found to breach NPP 1.1 on the grounds that its application was not limited to personal information which would be relevant to the claim in question. The insurer amended its forms so that only information relevant to a claim could be collected and by limiting the authority’s validity to the period during which a claim was being assessed. The investigation was closed on the grounds that the insurer had adequately dealt with the matter.

Surveillance

[3.49] *Complainant AE v Contracted Service Provider* [2006] VPrivCmr 6: This case was brought under the *Information Privacy Act 2000* (Vic). C’s wife (W) was the subject of surveillance in relation to a claim for compensation due to injury. In assessing the merits of the claim, a statutory authority used a private investigator (respondent) to collect information about W. C alleged that in collecting information about W, the respondent also collected information about him that was not necessary to assess the merits of W’s claim and that this breached IPP 1 (“Collection”). *Outcome:* The Victorian Privacy Commissioner held the relevant test was whether a reasonable person would find sufficient connection between the subject of surveillance and the other party (ie C). There was sufficient connection in this case and the collection was necessary.

***R v Company* [2009] PrivCmrA 21:** C was placed under surveillance by a company (CO) that had mistaken C for one of its employees. C had a relative who worked for CO and who had been on leave for

SAMPLE ONLY



Pages 1,015-1,035 are not part of this book preview.

specified parties, including D’s employer or accountant. IC phoned an employee of D’s business, asking about the nature of C and D’s relationship. No notification or authorisation had been provided or obtained in relation to such collection from the employee. *Outcome*: IC breached NPP 1.5 (as well as NPP 1.3) by failing to ensure that C had been made aware of the purpose for the collection of the information from the employee.

Complaint Determination No. 4 of 2004: A tenancy database operator (TDO) collected information about tenants from member real estate agents for inclusion in its database. TDO provided its member real estate agents with privacy collection notices to provide to tenants on its behalf, however, the notices were ambiguous and confusing. *Outcome*: TDO breached NPP 1.5 on various grounds as a result of its failure to satisfy NPP 1.3 notification requirements.

Seven Network v Media Entertainment and Arts Alliance [2004] FCA 637: The respondent union, which was conducting a campaign in opposition to an enterprise agreement, engaged a call centre to poll employees regarding the proposed agreement. The union had taken no steps to comply with NPP 1.5 and that the script used by the call centre did not comply with NPP 1.3. *Outcome*: The union was in breach of its NPP 1.5 obligations.

[3.260] NPP 2 – Use and disclosure

Publications, guidelines and related materials

- OPC, *Guidelines to the NPPs* (2001) at pp 35-42
- Case summaries under IPPs 10 and 11 regarding secondary uses and disclosures at [5.600] and [5.770] respectively.

Introduction

[3.265] NPP 2 is arguably the most important NPP in the sense that it regulates the purposes for which organisations may use and disclose personal information they have collected.

Generally, NPP 2.1 only permits personal information to be used or disclosed for the purpose for which it was collected (primary purpose). If an organisation wishes to use or disclose information for another purpose (secondary purpose), it must ensure that the secondary purpose is authorised by an exemption to NPP 2.1 (set out in the sub-sections to that principle).

It has been held that NPP 2 is concerned with “... a case where information obtained properly for one purpose is collaterally exploited for another purpose”: *Seven Network v Media Entertainment and Arts Alliance* [2004] FCA 637 at [53].

NPP 2 only applies in relation to personal information collected after 21 December 2001 – see [14.275].

Terminology – “use” vs “disclosure”

[3.270] A critical distinction in NPP 2 terminology to understand is the difference between the terms “use” and “disclosure”. Confusion as to the meaning of these terms often leads to misapplication of NPP 2.

A “use” of personal information occurs where the information is handled *internally* within an organisation (*NPPG* p 25). A “disclosure” occurs where information is sent to a third party *outside* the organisation (including contractors and related corporations) (*NPPG* p 23). It may also include confirming to a third party the correctness of information provided by that party: see *R v Internet Service Provider* [2005] PrivCmrA 17 at [3.315]. A disclosure does not, however, include providing personal information to the individual to whom it relates as this is “access” (regulated under NPP 6) (*NPPG* p 23).

The following examples involving a hypothetical organisation demonstrate and contrast uses and disclosures (the examples assume the organisation operates within a single corporate entity):

- sharing between departments – if personal information is passed from the organisation’s HR department to its in-house legal department, this constitutes a *use* of personal information;
- sharing with third party – if personal information is passed from the organisation’s HR department to external legal advisers in a law firm, this amounts to a *disclosure* of the information;

- transfers between offices – transfers of personal information between the organisation’s branch offices (including overseas offices) are uses, not disclosures (even though documents may, for example, be physically leaving one office and going to another), as they occur within the single legal entity (*note*: in the case of an overseas data transfer, this would not be regulated by NPP 9 (“Transborder data flows”) as that principle only applies where personal data is being sent overseas by an organisation to someone other than itself or the individual to whom the information relates).

In relation to disclosures within corporate groups, see [168].

[3.278]

2.1 An organisation must not use or disclose personal information about an individual for a purpose (the secondary purpose) other than the primary purpose of collection unless:

“Primary purpose of collection”

[3.280] The primary purpose of collection is the particular purpose for which information was collected by the organisation, even if the organisation intends to use the information for additional purposes (ExpMem1 note 320; *NPPG* p 35). For example, if a bank collects an individual’s personal information on a loan application form, the primary purpose of collection will generally be to provide financial services. Similarly, if a retailer collects personal information from a customer returning a faulty product for repair under a warranty, the primary purpose of collection would be to service the warranty.

If an organisation provides more than one product or service in a single transaction, the primary purpose attaches to each product or service such that, instead of there being more than one primary purpose, there is a single primary purpose to provide each product or service (*GPPHS* p 12).

Where personal information is collected from a person other than the individual concerned, the primary purpose of collection will generally be the purpose for which it is used in relation to the individual, eg where a business receives a tender application from a potential supplier and obtains information about the applicant from an industry member, the primary purpose of collection is to assess the applicant’s tender (see ExpMem1 note 320; *GPPHS* p 12).

In *Seven Network v Media Entertainment and Arts Alliance* [2004] FCA 637, the court considered whether a disclosure by a principal to an agent was for the primary purpose of collection. The respondent had engaged a call centre to poll employees regarding an enterprise agreement. The applicant argued that information disclosed by the call centre to the respondent was for an unrelated secondary purpose. *Gyles J* held (at [53]): “I am not satisfied that there is a primary and a secondary purpose in an agency situation like the present. If there is, then the better view is that the primary purpose is that of the principal ... In any event, if there are two purposes, they were directly related”.

It has been held under Victorian privacy legislation that, where a person lodges a complaint with an organisation about an individual, it is arguably part of the primary purpose of collection to show the complaint to the individual concerned in the interests of natural justice: *Complainant AG v Local Council* [2007] VPrivCmr 2.

Cases

***E v Private School* [2010] PrivCmrA 6:** C told a private school (S) they were considering legal action against S. S replied that it would defend any legal action. In an attempt to conciliate the matter, C sent S a copy of their intended legal claim. The Commissioner found that the primary purpose for which S collected the information was to defend, or avoid, any legal action brought by C.

“Primary purpose of collection” – health service providers

[3.285] Where a health service provider treats a patient in a single appointment for more than one unrelated injury or illness, the primary purpose attaches to each service such that there will be a single primary purpose to treat the patient for each injury or illness (see Priv. Cmsnr., *GPPHS* p 12).

This construction of the meaning of the “primary purpose of collection” is not wide enough to encompass, in addition to the episode of health care during which the information is collected, all future

episodes of health care for the patient. This is not consistent with a holistic approach to health care that many health service providers adopt whereby health information is used in the treatment of future injuries and illnesses from which the patient may suffer. In view of this, health service providers should obtain consent at the time of collection to use and disclose health information for future episodes of health care if relevant.

Publications, guidelines and related materials

- OPC, *Information Sheet 8 – Contractors* (2001)
- OPC, *Information Sheet 23 – Use and disclosure of health information for management, funding and monitoring of a health service* (2008)
- OPC, *Information Sheet 25 – Sharing health information to provide a health service* (2008)

Cases

Disclosures to family member/former spouse

[3.290] *J v Home Shopping Retailer* [2008] PrivCmrA 10: C purchased items from a home shopping retailer (R) as an unexpected gift for their spouse (S). S later telephoned R to purchase items and an employee disclosed to S that C had purchased items, revealing the nature of the gift. C and S approached R about the disclosure, seeking financial compensation for the stress and anxiety they suffered as a result of the disclosure and an undertaking that R would not discuss the matter with other employees, nor disclose their personal information to another party. C was dissatisfied with R’s response. *Outcome:* R resolved the matter by reminding staff about the impact of handling customers’ personal information, undertaking to monitor calls for quality and privacy matters, confirming that no record of the disclosure or the complaint was kept (preventing further discussion of the incident) and by issuing C a written apology and a substantial discount on the item that was to be a gift.

***E v Financial Institution* [2003] PrivCmrA 3:** Disclosure by a financial institution’s staff member of information about an account holder to the staff member’s family was held not to be covered by any of the exemptions under NPP 2.1. Further, while the institution could show when the information had been modified, an inability to show when it had been accessed by a staff member was held to result in an increased risk of breaching NPP 2.1. The Commissioner indicated that the organisation should take appropriate IT measures to ensure that access to financial information is monitored in the future.

***T v Private Community Centre* [2008] PrivCmrA 20:** C and their ex-spouse used a community centre for the handover of care of their children. C alleged that the centre had disclosed to their ex-spouse copies of letters C had sent to the centre. *Outcome:* There was no breach. The centre implemented a range of data security measures including a “clean desk” policy, storing client information in locked cabinets and drawers, and ensuring that personal information that was no longer required by the centre was securely disposed of. There was no evidence to show that C’s personal information had been disclosed to the ex-spouse.

***A v Licensed Club* [2007] PrivCmrA 1:** C was a member of a licensed club. Two individuals, one of whom was C’s ex-partner, told the club manager that they were friends of C and the manager disclosed C’s home address to them. C received phone calls which resulted in C feeling unsafe and relocating. C sought compensation for relocation costs and subsequent loss of income. A club representative failed to attend a meeting arranged with C to address the complaint. *Outcome:* The club agreed to pay C an undisclosed amount of compensation in settlement of the complaint.

***P v Electrical Goods Retailer* [2006] PrivCmrA 15:** C paid a retailer (R) a deposit for a fridge which was to be delivered once the balance was paid. However, the fridge was delivered to C’s house before the balance was paid. C did not pay the balance and refused to return the fridge. Several months later the husband (H) of the sales person (SP) who took the deposit attended C’s residence on two occasions requesting that C return the fridge or pay the outstanding money. Later, SP and H attended C’s residence. SP claimed that she was being threatened with dismissal over the incident. C alleged that R had interfered

with their privacy by using their personal information to seek payment for or return of the refrigerator and by disclosing their information to H during R's attempts to obtain the return of the refrigerator. *Outcome:* Use of C's information for the purpose of attempting to recover the outstanding debt did not breach NPP 2.1. Such use was directly related to the primary purpose of the collection. Further, whilst C may not have expected SP themselves to attend C's house, they would have reasonably expected a representative from R to contact them in relation to the debt (*editorial note:* this is most likely a reference to the exemption under NPP 2.1(a)). The disclosure to H breached NPP 2. R claimed it was not responsible for the disclosure as it had not been aware of it. This argument was rejected as R was vicariously liable under s 8(1)(a). R also argued that the disclosure was permitted under NPP 2.1(f) as being a disclosure as part of an investigation of unlawful activity; however, this was also rejected as H "was not an employee" of R (although NPP 2.1(f) does not require disclosure to an employee) and, as R had not been aware of H's involvement, C's information could not have been disclosed as a part of R's investigation. The parties agreed on a confidential settlement.

U v Major Banking Institution [2003] PrivCmrA 19: The respondent breached NPP 2.1, as well as s 18N(1) of the credit reporting provisions of the Privacy Act, by disclosing a default notice regarding C's overdue bank account to C's spouse from whom she was separated. The respondent indicated that it was unaware of C's changed circumstances, resulting in out-of-date information remaining on its database, and apologised. *Outcome:* The apology was deemed an appropriate response by the Commissioner and, accordingly, a claim for compensation was not substantiated.

Linked accounts

[3.295] *K v Financial Institution [2003] PrivCmrA 9:* K and X held accounts with a financial institution. The organisation erroneously linked K's account with that of a family member, X, and subsequently disclosed information about K's favourable financial position to X. Based on this information, X requested K to guarantee certain financial dealings which K felt they could not refuse due to the nature of their relationship with X. K sought compensation for the anxiety of having to provide X with financial support. *Outcome:* The disclosure of K's information by the organisation was held to be a potential breach of NPP 2.1. The organisation apologised, provided additional staff training and paid compensation of \$1,000.

D v Insurance Company [2007] PrivCmrA 6: C's insurance company (IC) had been including C's personal information on the accounts of a third party (TP) without C's knowledge. After being contacted by C, IC amended its records so that C's information was no longer visible on TP's accounts, apologised for the inconvenience and offered an ex gratia payment of \$750. C was dissatisfied with this proposed resolution claiming that IC had not taken steps to ensure that information would not be similarly disclosed in the future and that the payment offered was insufficient. C wanted IC to amend its business practices. *Outcome:* The Commissioner referred the complaint to IC in order for it to further consider the issues raised. IC counselled staff members involved and circulated a notice to all call centres and branches reminding them of their obligations under the Privacy Act. IC again offered an apology to C and an increased ex gratia payment of \$1250 which were accepted by C.

Records in public place

[3.300] *J v Superannuation Provider [2005] PrivCmrA 7:* C claimed that records relating to a claim against his super fund provider were found on a public thoroughfare, including reports about covert surveillance undertaken as part of the claim assessment, and that information about him was disclosed to his neighbours (assumedly as part of the surveillance). The contracted surveillance company stated that information was not disclosed to his neighbours. *Outcome:* In the absence of any evidence to the contrary, the super provider had not, on the balance of probabilities, breached NPP 2.1.

Facsimile transmissions

[3.310] *OPC v Banking Institution [2005] PrivCmrA 11:* The respondent, a banking institution, had an internal fax number for receiving customer information from staff. Staff occasionally mis-keyed the fax

SAMPLE ONLY



Pages 1,050-1,112 are not part of this book preview.

Health service providers

[3.960] *NK v Northern Sydney Central Coast Area Health Service (No.2)* [2011] NSWADT 81: NK was a mentally ill patient who worked at a hospital operated by the respondent, a NSW public sector agency. Whilst presenting at the hospital’s emergency department in relation to anxiety and stress, NK told Nurse W that he had thoughts of harming himself or a colleague at the hospital who he considered had bullied him, but was assessed as at low risk of doing either. Information subsequently recorded in NK’s medical file was found to be inaccurate. Nurse W reported NK’s admission to the hospital’s HR Manager, without checking the accuracy of the information provided, on the basis that NK posed a threat to staff. The HR Manager suspended NK from work, blocked his hospital access card and directed that he only be allowed into the hospital as a patient or for meetings concerning his suspension. As a result NK felt unable to seek further medical help from the hospital (which was also his local hospital) for reasons including fear that his personal information would be again used against him. These events led to NK attempting suicide. *Outcome:* The NSW Administrative Decisions Tribunal awarded the applicant, NK, the maximum compensatory damages possible of \$40,000 for breaches of the *Privacy and Personal Information Protection Act 1997* (NSW) (PIIP Act) and *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act). The conduct of the hospital was held to have amounted to an oppressive disregard of NK’s privacy. In addition to awarding maximum damages, the court stated: “NK can never be adequately compensated for the loss that he has suffered. I encourage the Respondent to consider other options that may be available to it to provide additional support to NK in that regard.” The court found that Nurse W and the HR Manager failed to check the accuracy of NK’s personal information before using it in various ways that had extremely serious consequences for NK’s health and employment. The Tribunal found that the hospital had not demonstrated good faith towards NK.

[3.990] NPP 4 – Data security

[3.993]

4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.

Publications, guidelines and related materials

- OPC, *Information Sheet 6 – 2001 Security and Personal information*
- OPC, *Guidelines to the NPPs* (2001) at pp 44-45
- RACGP, *Computer security guidelines: A self assessment guide and checklist for general practice* (3rd ed)
- OICQ, *Information sheet – Personal information and network security – lessons from the Auditor-General’s report*
- AS/NZS ISO/IEC 27001:2006 *Information technology – Security techniques – Information security management systems – Requirements*
- AS/NZS ISO/IEC 27002:2006 *Information technology – Security techniques – Code of practice for information security management*
- AS ISO 15489.1 – 2002 *Records management – General*
- AS ISO 15489.2 – 2002 *Records management – Guidelines*

Overview

[3.995] NPP 4.1 aims to ensure that information is not mishandled or used for unauthorised purposes by requiring organisations to take appropriate security measures to protect it. Data security measures need to encompass both hardcopy and electronic records.

Data security – commentary and practical guidance

[3.1000] Detailed commentary on data security issues is set out at [205], including on:

- what constitutes “reasonable steps” to secure information (at [205.20]);

- relevant security standards (at [205.30]);
- checklist of data security risks and control measures (at [205.40]);
- portable storage devices, such as laptops and USB flash drives (at [205.70]);
- data security breaches and notification (at [205.85]).

Cases

Unauthorised staff access

[3.1005] *E v Financial Institution* [2003] PrivCmrA 3: A financial institution's staff member accessed information about an account holder and disclosed it to the staff member's family. While the organisation kept records of when a transaction modified or deleted information relating to the account, it did not keep logs of when the information was accessed without modifying the information. The organisation could only provide limited assurances about whether the account information was protected against unauthorised access, misuse or disclosure. *Outcome:* The conduct did not breach NPP 4.1 on technical grounds as it occurred before the commencement of the NPPs. However, the Commissioner indicated that the organisation should take appropriate IT measures to ensure that access to financial information is monitored in the future.

***NS v Cmsnr, Dept of Corrective Services* [2004] NSWADT 263 revised – 14/01/2005:** An employee of a NSW agency had accessed client information for personal reasons and disclosed it to third parties. The agency had flagged all relevant information with a notice stating that it is confidential and must not be used for personal reasons. *Outcome:* The agency's computer flag was an adequate security safeguard and, as such, the agency did not breach s 12 of the *Privacy and Personal Information Protection Act 1998* (NSW) which established equivalent data security obligations to those under NPP 4.1.

***N v Utility Provider* [2006] PrivCmrA 13:** C alleged that a utility provider (UP) improperly disclosed and failed to secure their personal information against unauthorised access and disclosure. C alleged their ex-partner (EP), an employee of UP, improperly accessed their accounts in order to ascertain information about their assets and that EP improperly disclosed this information to a third party. UP could not ascertain whether EP had improperly accessed the account because it did not keep an audit trail recording staff access to customer records. There was no evidence that EP had improperly disclosed C's information which could have come from other sources. C was unable to provide substantive evidence to support their claim that their information had been inappropriately disclosed by UP. UP argued it had taken reasonable steps to protect the information against misuse and loss, or from unauthorised access, modification or disclosure, as required under NPP 4.1. It advised that it complied with the relevant Australian Standard and with its own procedures. *Outcome:* In view of the fact that UP held a large amount of personal information and that the type of information required to establish accounts was extensive, the information should be afforded a high level of protection, especially given the possible serious consequences of any unauthorised access. The absence of an audit trail in a large automated billing system which can identify access to customer accounts meant that UP had breached NPP 4.1 by failing to take adequate steps to protect C's information against misuse and loss, and from unauthorised access, modification or disclosure. UP agreed to implement password security to protect C's account information.

***X v Transport Company* [2007] PrivCmrA 26:** C was a contract worker for a transport company (TC). C alleged that TC failed to secure the results of a medical assessment C had undergone and had disclosed information about the assessment to employees. *Outcome:* No evidence relating to security processes was presented other than C's allegations, so it was not possible to determine whether TC had complied with NPP 4.1. However, the Commissioner advised TC to adopt additional security measures to minimise the possibility of such incidents occurring in the future.

Unauthorised staff disclosure

[3.1010] *H v Health Service Provider* [2007] PrivCmrA 10: C underwent a medical test at a medical centre (MC). An employee of MC disclosed the results to a third party. The employee was reprimanded by MC. However, C was not satisfied with this outcome. MC's standard records handling procedures included

SAMPLE ONLY



Pages 1,115-1,201 are not part of this book preview.

Annotated Information Privacy Principles

[5.10] Principle 1 – Manner and purpose of collection of personal information

1. Personal information shall not be collected by a collector for inclusion in a record or in a generally available publication unless:
 - (a) the information is collected for a purpose that is a lawful purpose directly related to a function or activity of the collector; and
 - (b) the collection of the information is necessary for or directly related to that purpose.
2. Personal information shall not be collected by a collector by unlawful or unfair means.

Publications, guidelines and related materials

- OPC, *Plain English Guidelines to IPPs 1-3*

Overview

IPP 1 generally provides that personal information that is collected must be:

- necessary for a function or activity; and
- collected lawfully and fairly.

IPP 1.1 means that an agency cannot collect information for which it has no current or planned future need. One way in which agencies often breach this principle is by requesting irrelevant information from customers on application forms, either because the question directly requests irrelevant information or, more commonly, because the question is drafted too broadly such that the details requested are not limited to those which are relevant to the purpose for which the information is required. For example, a licence application form might request “have you ever had any serious injury, illness, operation or been in hospital for any reason?”, whereas the question should generally be restricted so it relates solely to conditions that are relevant to injuries, illnesses and other conditions that impact on the applicant’s ability to undertake activities pursuant to the licence.

However, where personal information is collected in the context of providing a particular service, IPP 1 does not mean that the agency cannot request information for other purposes at the same time. For example, a social welfare benefit application form may request information relating to other activities undertaken by the relevant agency. Whilst that other information will not be needed for application assessment purposes, the information is “necessary” for the other activities the agency conducts and its collection will therefore generally be permitted under IPP 1.

Collection – IPPs 1-3

[5.15] Collection of personal information is regulated under IPPs 1-3, including what information may be collected, how it may be collected, notification requirements (eg privacy notices that must be provided) and purposes for which information may be collected. Agencies collect personal information using a large number of methods, both formal (eg application forms) and informal (eg via email). Requirements under IPPs 1-3 need to be considered and applied in the context of *all* methods of collection, not just the most common or formal methods, such as through application forms.

It is a relatively common misconception that agencies cannot collect information from private sector organisations or, at least, that different requirements apply in these circumstances. However, there is no difference in obligations in regards to whether an entity from which information is being collected by an agency is in the public sector (ie another agency) or the private sector (eg an employment agency, a private sector law firm, a GP or an individual). IPPs 1-3 apply in the same way to both types of collection.

When is personal information “collected”?

[5.20] An agency “collects” personal information when it:

- asks for and receives the information either from the individual concerned (eg on a form) or a third party (eg another agency); or
- is given the information unsolicited (eg in a letter of complaint).

“Purpose” of collection?

[5.25] The Privacy Commissioner generally defines the “purpose” of collection of personal information narrowly and from the point of view of what a reasonable person would conclude in the circumstances. It is the specific reason for which the information is being collected in the relevant instance. It is not something broad, such as to administer a set of laws (*IPPG* 1-3 at p 6). For example, if Centrelink collects an individual’s personal information through an online claim form for Youth Allowance, the “purpose” of collection would generally be to assess the individual’s eligibility for Youth Allowance benefits. It would not be a broad purpose, such as to deliver welfare services.

“Necessary for” and “directly related to” the purpose of collection

[5.30] Information is “necessary for” and “directly related to” the purpose of collection when it directly helps to achieve that purpose (*IPPG* 1-3 at p 6). The information collected does not need to be indispensable (eg an activity could not be conducted without it). However, information is not “necessary” or “directly related” simply because it might be useful at some time in the future (see the commentary regarding similar terminology in the NPPs at [3.45]). These requirements place significant limitations on the types of information agencies can collect and therefore handle. For examples of unnecessary collections that may breach IPP 1.1, see *IPPG* 1-3 at pp 6-7.

It is *not* sufficient that consent is obtained for collection. Whether consent is present is irrelevant to the question of whether information is “necessary” for the relevant purpose.

Cases

Collection forms

***Own Motion Investigation v Australian Government Agency* [2007] PrivCmrA 4:** An online form provided by an agency for job applicants asked applicants to advise whether they had ever suffered from a work-related injury or illness. The collection of information was not required by any law nor was it relevant to the process of recruitment and selection. *Outcome:* The Commissioner didn’t make a formal finding, but indicated the collection was not necessary (and, as such, was likely to have been a breach). The agency amended its recruitment practices accordingly and verified that no applicant had been disadvantaged by the collection.

***JK v Department of Transport Infrastructure Development* [2009] NSWADT 307:** C, a bus driver, was required to submit a completed Medical Assessment Form to renew his public passenger vehicle driver’s licence. The form asked: “Have you ever had any serious injury, illness, operation or been in hospital for any reason? Yes No If yes, give details”. *Outcome:* The information required in response to the question was not reasonably necessary for the purpose of determining whether an applicant met the relevant medical fitness criteria and breached HPP 1 (equivalent to IPP 1) of the *Health Records and Information Privacy Act 2002* (NSW). The question “cas[t] a very wide net” and was designed to capture information in relation to any serious injury, illness, operation which an applicant has ever had, irrespective of its relevance to medical fitness to drive a public passenger vehicle. The question sought details of every time an applicant had been in hospital, irrespective of the relevance of that information to fitness to drive.

Employee monitoring

***Griffiths v Rose* [2011] FCA 30:** The applicant, an employee with a Commonwealth Government department, had had his employment terminated for using a work laptop at home outside of business

hours using his own internet service provider (ISP) to view pornography in breach of the workplace Information and Communications Technology (ICT) Policy and, in turn, the Australian Public Service Code of Conduct which required compliance with that policy. The Department discovered the access as a result of software it had installed on the laptop which monitored internet activity, including websites visited. The software logged keyword searches and took desktop screenshots every 30 seconds which were relayed to a dedicated server. The applicant sought orders quashing the decisions that he had breached the Australian Public Service Code of Conduct and that the appropriate sanction was termination of his employment. The applicant argued the Department had breached IPP 1(1) on the basis that the information collected relating to his personal use of the laptop outside of work using his own ISP was not necessary for any purpose of the Department. *Outcome:* The Department did not breach IPP 1(1) as the collection of information was necessary to monitor compliance with the Code of Conduct. The Department had a legitimate interest in ensuring its equipment did not come into contact with pornography, a specific concern being the risk posed by the pornography's accidental reappearance or display in the workplace.

When is a collection “unfair”?

[5.35] For commentary regarding the meaning of “fair”, see [3.65] under NPP 1.2 (equivalent to IPP 1.2).

Cases

Griffiths v Rose [2011] FCA 30: The applicant, an employee with a Commonwealth Government department, had had his employment terminated for using a work laptop at home outside of business hours using his own internet service provider to view pornography in breach of the workplace Information and Communications Technology (ICT) Policy. The Department discovered the access as a result of software it had installed on the laptop which monitored internet activity, including websites visited. The software logged keyword searches and took desktop screenshots every 30 seconds which were relayed to a dedicated server. The ICT Policy notified employees that monitoring of ICT facilities would occur and the applicant had signed a document recording that he understood the ICT Policy. The applicant argued the Department had breached IPP 1(2) on the basis that the method of collection was unfair. *Outcome:* The Department did not breach IPP 1(2). The monitoring and collection were not unfair as the Department had notified the applicant that this would occur through the ICT Policy and the applicant had acknowledged he understood this policy.

F v Contract Service Provider to a Commonwealth Government Agency [2011] PrivCmrA 6: A Commonwealth agency contracted CSP for the purpose of conducting an investigation about C concerning an allegation that C had behaved inappropriately during a meeting with a third party. CSP collected personal information about C from a third party by correspondence and through an interview. C claimed the investigation was unlawful on the basis it contravened discrimination legislation and that, consequently, collection of information about him from the third party was unfair and breached IPP 1. *Outcome:* The collection was not unfair, nor was it unreasonably intrusive. C had not been deceived or misled in any way.

V v Commonwealth Agency [2008] PrivCmrA 22: C provided a letter of support for their partner in regards to an application by the partner for an agency service. The agency interviewed C. The partner's application was granted. Later, a law enforcement agency informed the agency that C's statements were inaccurate. Providing false or misleading information to the agency was an offence. The agency investigated C's conduct and asked C to attend a second meeting. Prior to the second meeting, agency officers informed C of the reason for the meeting, of the legal authority under which C's information was being collected and offered C the opportunity not to participate. C claimed they believed the second meeting was to discuss their partner's application (rather than their own conduct) and that collections of information during the meeting were unfair. *Outcome:* The Commissioner was satisfied that the agency informed C of the reason for the second meeting as per its version of events and, accordingly, found the resulting collections were fair and in accordance with IPP 1.2. If the agency had not so informed C, the collections may have been unfair.

For case summaries regarding “fair” collections under NPP 1.2 (equivalent to IPP 1.2), see [3.65].

SAMPLE ONLY



Pages 1,205-1,242 are not part of this book preview.

[5.628]

- (a) the individual concerned has consented to use of the information for that other purpose;

Scope and operation

[5.630] IPP 10(a) is one of the most widely used exemptions to IPP 10 as it permits use of information for any purpose for which consent is obtained. Accordingly, if an agency is aware consent will be required to use information for a particular purpose, written consent for such use should be obtained at the time of collection (eg through terms of service or consent forms).

Consent

[5.655] Detailed commentary on consent is set out at [126], including:

- constituent elements of consent at [126.20];
- obtaining consent at [126.45];
- bundled consents at [126.85];
- drafting consent forms at [126.95];
- types of consent that should be obtained at [126.105].

[5.663]

- (b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;

Scope and operation

[5.665] The Commissioner has indicated that this exemption (and the exemption under IPP 11.1(c)) should only be relied upon in emergencies. The exemption could, for example, permit an agency to use (or, in the case of IPP 11.1(c), to disclose) information about an individual's whereabouts to police or health care workers where an individual suffering a mental illness is missing, incapable of taking care themselves and in need of regular medication.

For detailed guidance on the application of this principle, see *IPPG* pp 37-39.

[5.673]

- (c) use of the information for that other purpose is required or authorised by or under law;

“Required” vs “authorised” by law

[5.675] “Required” means the agency has no discretion in the matter. “Authorised” means the agency does have discretion to decide whether it uses (or discloses) the information for the relevant purpose.

A use of information is usually *required* by law if legislation governing the agency (see *IPPG* p 42):

- specifically requires it to use the information for the secondary purpose; or
- requires the agency to perform a specific function which necessarily requires the agency to use the information for the secondary purpose.

A law *authorises* a use (or disclosure) for a secondary purpose if it provides (see *IPPG* pp 42-44):

- express authority –
 - for example:

- an agency’s governing statute clearly and specifically gives it a discretion to use (or disclose) the information for that purpose;
- a statute specifically provides the relevant use (or disclosure) is permitted under the IPPs – for example, the *Australian Passports Act 2005* (Cth) provides:
 - s 42(1) – the Minister may request certain authorities to disclose information about an applicant for, or holder of, an Australian passport;
 - s 42(3) – for the purposes of IPP 11(1)(d), such a disclosure is deemed to be “required or authorised by law”;
- however, general statutory powers that are granted to office holders to do anything necessary or convenient for the performance of their functions are not sufficient.
- implied authority –
 - a statute requires or authorises a function, activity or scheme that clearly and directly entails the use (or disclosure), ie it is essential to effect the function, activity or scheme;
 - the Commissioner has indicated implied authority would be present in the following examples (in relation to disclosures) (*note*: the Commissioner has adopted a broad interpretation in this regard):
 - if an industrial law requires a union to conduct an election by postal ballot for all people in a workplace, this impliedly authorises an employer agency to disclose to the union the names and addresses of its non-union employees;
 - if an agency has statutory authority to obtain personal information about an individual, the agency may, when requiring information from a third party, inform the third party of the individual’s name in order to identify the person to whom the request relates.

What constitutes “law”?

[5.680] The Privacy Commissioner has expressed the view that “law” for the purposes of IPP 10.1(c) generally means a Commonwealth law, such as (*IPPG* p 40):

- Commonwealth Acts (eg an agency’s governing statute);
- Commonwealth delegated legislation (eg regulations and determinations);
- documents given the force of Commonwealth law (eg breaches can result in an offence being committed or the imposition of a penalty), usually by another statute – eg industrial awards.

The Commissioner has indicated that “law” may, in certain circumstances, also include State or Territory laws that bind the Commonwealth, eg subpoenas and warrants issued by State courts. In response to the ALRC’s privacy review, the Government has indicated that it intends to clearly define the meaning of “law” in the Privacy Act to include, among other things, State legislation and the common law.

The Commissioner has expressed the view that “law” under IPP 10.1(c) generally does not include (*IPPG* p 40):

- State Acts (subject to the exception above);
- information requests from foreign governments;
- common law;
- Cabinet decisions;
- contractual agreements (unless given force of law by a statute).

[5.688]

- (d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or

SAMPLE ONLY



Pages 1,245-1,246 are not part of this book preview.

[5.770] Principle 11 – Limits on disclosure of personal information

Publications, guidelines and related materials

- OPC, *Plain English Guidelines to IPPs 8-11*
- Case summaries under NPP 2 regarding secondary disclosures at [3.260]

Overview

IPP 11 generally provides that information must not be disclosed for any reason, unless permitted under an exemption to IPP 11.1.

Scope and operation

[5.775] IPP 11 is structured in the following way:

- it prohibits all disclosures of a person's personal information other than to the person concerned;
- it then sets out a series of exemptions which permit certain disclosures.

IPP 11 provides a simple framework within which to assess whether a disclosure of information is permitted in any given circumstances.

Disclosures to private vs public sector entities – is there a difference?

[5.780] Many agencies primarily make disclosures to other agencies. However, it is often necessary for agencies to make disclosures to private sector entities; for example, to:

- contracted service providers;
- workers' unions;
- health service providers;
- employment agencies; and
- legal advisers.

The requirements regarding the purposes for which a disclosure may be made are the same, regardless of whether the entity to which the information is being disclosed is in the private or public sector. As such, provided the disclosure is permitted by one of the exemptions to IPP 11.1, it is irrelevant whether the receiving entity is in the private or public sector.

Cases

Disclosure to another agency

[5.785] *M v Commonwealth Agency [2003] PrivCmrA 11*: C worked for Agency A and, following a workplace injury, lodged a claim with Agency B, responsible for providing assistance. C signed a declaration authorising disclosures of information to other parties involved in the management of the injury. C provided Agency B with a medical certificate and information to the effect that a condition was exacerbated by employment with Agency A. Agency B's governing legislation authorised a person to provide to Agency B certain information it requested. Agency A provided information from C's doctor to Agency B and, following a request from Agency B, provided other information. C alleged that these disclosures by Agency A were not authorised. *Outcome*: The disclosure was permitted under several exemptions. These were:

- IPP 11.1(a) (regarding disclosures an individual is reasonably likely to be aware of) – As the claim specifically related to damage caused at work, C was reasonably likely to be aware that information relevant to the claim would be disclosed to Agency B.
- IPP 11.1(b) (regarding disclosures with consent) – C provided implied consent by a combination of signing the declaration authorising disclosures and stating that the injury was exacerbated by her employment.

- IPP 11.1(d) (regarding disclosures authorised by law) – The disclosure of the “other information” provided by Agency A upon request was authorised under Agency A’s governing legislation and, as such, was permitted under IPP 11.1(d).

Disclosure to family member/relative/former spouse or partner

X v Commonwealth Agency [2004] PrivCmrA 4: C was assisted at an agency counter by an employee who was formerly related to C. C advised the agency that C was expecting to receive money from a court settlement. The agency’s employee disclosed this information to C’s ex-partner. The next day, C’s ex-partner obtained a court order restraining C from accessing that money. *Outcome:* The Privacy Commissioner formed the view that no relevant exemption under IPP 11 applied and, therefore, the agency had breached IPP 11. However, the agency did not accept that it had disclosed C’s personal information (perhaps on the grounds that it denied vicarious liability for the employee’s actions in this instance on the basis that they were not done in the performance of their employment duties – although this is not known). C wished to pursue the matter in court and the Commissioner closed the investigation without a conciliated result.

L v Commonwealth Agency [2008] PrivCmrA 12: C’s former spouse (S) submitted an application form to an agency in which they included C’s address. An agency inadvertently applied the address of C’s former spouse (S) to C’s records, resulting in mail intended for C being sent to S. Legal action ensued between C and S in relation to the information that was disclosed. *Outcome:* The agency acknowledged that its error, committed in breach of IPPs regarding data accuracy and disclosures, had contributed to the legal costs incurred by C. In view of this acknowledgement, the matter went to conciliation. A confidential settlement was reached, including part payment of C’s legal costs and a further amount for injuries to C’s feelings.

P v Commonwealth Agency [2009] PrivCmrA 19 P v Commonwealth Agency [2009] PrivCmrA 19: C left their marital home due to domestic violence. C moved to a residence which was subjected to break-ins and a violent attack. Because of safety fears, C moved again. To diminish the risk of harm, C changed their name by deed poll and concealed the new address from the ex-partner. C was a client of a Commonwealth agency. C advised the agency of the new address and change of name, requesting the information remain confidential. The agency sent a letter to C, containing references to C’s new name and address, at C’s marital home. C’s ex-partner viewed this information and contacted C. The agency acknowledged the disclosure was not permitted under IPP 11, apologised and offered to pay an amount in compensation, which C rejected. *Outcome:* C sought compensation for health treatment and other costs incurred after the disclosure and for injury to feelings. The agency agreed to pay some compensation but not the amount requested by C. C provided further evidence to support their claim for compensation. The agency offered an increased monetary sum which C accepted in settlement of the matter.

Disclosure to new employer

M v Australian Government Agency [2005] PrivCmrA 10: C was employed by an agency and was being investigated by the agency regarding alleged misconduct. C resigned before the investigation was finalised and began working for a new employer. One of the agency’s employees disclosed information concerning the investigation to the new employer. *Outcome:* The disclosure breached IPP 11 as none of the exemptions under IPP 11.1 permitted the disclosure. The agency provided C with a formal written apology and an explanation of the findings of its investigation regarding the improper disclosure.

[5.793]

1. A record-keeper who has possession or control of a record that contains personal information shall not disclose the information to a person, body or agency (other than the individual concerned) unless:
 - (a) the individual concerned is reasonably likely to have been aware, or made aware under Principle 2, that information of that kind is usually passed to that person, body or agency;

Scope and operation

[5.795] It is not necessary to check that the person is *actually* aware. The requirement under IPP 11.1(a) is that the person is “reasonably likely to have been aware, or made aware” under IPP 2. If this is so, then, even if the person isn’t actually aware, IPP 11.1(a) requirements will have been met.

“Reasonably likely to have been aware”

[5.800] Generally, people are not familiar with the internal workings of agencies and their disclosure practices, so an agency should not readily assume such knowledge.

Relevant considerations in assessing likely awareness of disclosures may include:

- the nature of the relationship between the person and agency – eg their level of familiarity with the agency’s practices;
- the person’s professional experience – eg mechanic vs a government lawyer.

To be “reasonably likely to have been ... made aware under Principle 2”, the Privacy Commissioner has indicated that the person must have been given an IPP 2 privacy collection notice (*IPPG* p 33). Accordingly, agencies should ensure that IPP 2 privacy collection notices clearly state any disclosures that are likely to occur. If this is done, it generally won’t be necessary to request consent for the disclosure.

Cases

[5.805] *Maman v Minister for Immigration* [2011] FMCA 426: The applicant had applied for a visa. As part of this process, the applicant’s wife from whom the applicant had separated, had written a letter containing personal information to the Department processing the visa application. The applicant sought access to the letter, but the Department refused the request on the basis that it contained personal information about a third party who would not be reasonably likely to have been aware that the information would be disclosed to the applicant. *Outcome*: The wife was not likely to have been aware that the letter was of a type that was usually passed to the visa applicant and access could be denied.

C v Commonwealth Agency [2003] PrivCmrA 1: C, a Commonwealth agency employee, applied for work at another agency and named their supervisor as a referee. The relevant position was primarily as a call centre operator. The supervisor disclosed to the interview panel that C suffered from epilepsy and depression, was on sick leave and did not cope well under stress. C’s application was unsuccessful. C claimed this was due to the disclosures by the referee and lodged a complaint about the disclosures. *Outcome*: The disclosure of information about epilepsy and sick leave breached IPP 11.1(a). C was not reasonably likely to be aware that the referee would disclose medical information in the course of providing a reference. The disclosure regarding C’s ability to cope with stress did not breach IPP 11 as this information was relevant to employment, particularly for a position as a call centre operator. C was reasonably likely to be aware that judgements of this kind could be conveyed by the referee. The agency apologised to C and paid compensation of \$7,000.

N v Australian Government Agency [2005] PrivCmrA 12: C sent two emails to an agency alleging a third party, an agency affiliate that received agency funding, had misused funds. The agency’s privacy policy stated that email messages provided to it would not be disclosed without the sender’s consent. Despite this, an officer of the agency forwarded the two emails to the third party. The third party instituted defamation proceedings against C on the basis of the emails. The parties reached a settlement out of court. *Outcome*: The agency was not entitled to rely on IPP 11.1(a) to justify the disclosure to the third party. In view of the agency’s privacy policy (which required consent for disclosure), C could not have been reasonably likely to have been aware that the emails would have been forwarded to the third party. The fact that C had sent one of the emails to other entities in addition to the agency did not negate the agency’s responsibility to comply with its privacy policy.

J v Commonwealth Agency [2009] PrivCmrA 13: C was an employee of an agency. The agency had undertaken an investigation into C’s conduct. C later submitted a workers’ compensation claim and the agency arranged for a doctor to assess C to determine their fitness for duties. The agency notified C that the purpose of the doctor’s appointment was to assess their ability to return to the workplace and that it

would provide the doctor with personal information about C. The information subsequently provided by the agency to the doctor included information relating to the investigation. The subject matter of the investigation was relevant to the assessment of C's condition. C claimed the agency had no need to disclose this information. *Outcome:* The disclosure was permitted under IPP 11.1(a). C was reasonably likely to have been aware (even if not actually aware) that the information would be passed to the doctor because of the prior notifications they had received. It is usual practice in workers compensation matters for an employer to provide an assessing doctor with all relevant information about the employee. As the subject matter of the agency's investigation may have presented a barrier to C returning to work, the information was relevant to the assessment of C's condition.

[5.813]

- (b) the individual concerned has consented to the disclosure;

What constitutes "consent"?

[5.815] For commentary on what constitutes consent, see under IPP 10.1(a) at [5.635].

Where information relates to more than one individual, the consent of each person concerned is needed – see [126.95].

Disclosures to individuals' agents and authorised representatives

[5.820] Often, people will operate through agents and authorised representatives, such as lawyers and family members. Generally, documents can be disclosed to such representatives. However, the agency should first:

- verify the existence of the person's authority to act as agent or authorised representative – eg directly with the person concerned or by requesting a copy of a letter of authority;
- ascertain the scope of the consent for disclosure to determine what information can be given – this will depend on the nature and extent of the authority provided to the third party; for example:
 - if a person is dealing through a representative pursuant to a power of attorney – the agency could ask for a copy of the power of attorney which should expressly state the matters in relation to which the attorney is empowered to act;
 - if an agency is negotiating with a person's solicitor in regards to a personal injury settlement – it would be reasonable for the agency to disclose to the lawyer information relating to the claim but not information relating to a previous unrelated dispute the person had with the agency.
- verify the representative's identity.

Cases

[5.825] *C v Commonwealth Agency* [2003] PrivCmrA 1: C, a Commonwealth agency employee, applied for work at another agency and named their supervisor as a referee. The relevant position primarily involved answering phone enquiries. The supervisor disclosed to the interview panel that C suffered from epilepsy and depression, was on sick leave and did not cope well under stress. C's application was unsuccessful. C claimed this was due to the disclosures by the referee and lodged a complaint about the disclosures. *Outcome:* The disclosure of information about epilepsy and sick leave breached IPP 11.1(b). By asking the supervisor to act as referee, C had impliedly consented to them disclosing to the interview panel information relating to skills, work experience and personal attributes relevant to the advertised position. However, C had not consented to disclosures regarding medical conditions and past sick leave taken. The agency apologised to C and paid compensation of \$7,000.

N v Australian Govt Agency [2005] PrivCmrA 12: C sent two emails to an agency containing allegations of a misuse of funds by a third party, an affiliate of the agency to which the agency provided funding. The agency's privacy policy stated that email messages provided to it would not be disclosed without the sender's consent. Despite this, an officer of the agency forwarded the two emails to the third party. C had

SAMPLE ONLY



Pages 1,261-1,402 are not part of this book preview.

Annotated Draft Australian Privacy Principles

PRIVATE SECTOR ANNOTATIONS

[7.100] APP 1—open and transparent management of personal information

(1) The object of this principle is to ensure that entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

(2) An entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity’s functions and activities that:

- (a) will ensure that the entity complies with the Australian Privacy Principles; and
- (b) will enable the entity to deal with inquiries or complaints from individuals about the entity’s compliance with the Australian Privacy Principles.

Purpose (APP 1(2))

[7.105] The Government’s *Companion Guide – Australian Privacy Principles* (June 2010) outlines the purpose of APP 1 as follows (at 9):

The requirement for open and transparent management ... will emphasise that entities should first plan *how* they will handle personal information before they collect and process it.

The principle is also intended to outline that part of complying with the Australian Privacy Principles is making sure that entities consider their privacy obligations when planning new systems.

This is part of international moves towards a “privacy by design” approach, that is, ensuring that privacy and data protection compliance is included in the design of information systems from their inception. (emphasis in original)

Accordingly, APP 1(2) aims to ensure that entities take a *proactive* approach to privacy compliance (ie foreseeing privacy risks and putting systems in place to avoid such risks eventuating), rather than a *reactive* one (eg resolving privacy issues and complaints as they arise, resulting in privacy policies and procedures being developed piecemeal).

Equivalent NPPs

[7.110] Obligations to have compliance systems in place under APP 1(2) have no *express* equivalent under the NPPs (although the need for such systems is, for many organisations, a practical requirement in order to comply with the NPPs).

Impact of changes (APP 1(2))

Level of impact: medium

(i) Measures to ensure compliance (APP 1(2)(a))

[7.115] Whilst the NPPs do not contain an express requirement that an organisation must take reasonable steps to implement practices, procedures and systems to ensure compliance with the NPPs, many organisations already have in place such measures as part of their privacy compliance programs. For such organisations, APP 1(2)(a) will have little impact as it is merely formalising practical measures already implemented.

However, APP 1(2)(a) will have ramifications for organisations that have *not* adopted practices, procedures and systems to ensure compliance where it would be reasonable for them to do so. Organisations that fall within this category may include:

- medium size businesses;
- small businesses (with a turnover of less than \$3m) that trade in personal information;
- small health service providers (eg medical centres); and

- large organisations which:
 - have adopted a risk-management strategy to address privacy issues as they arise; or
 - have opted not to invest resources in developing privacy compliance regimes based on a view that privacy is not a sufficiently relevant compliance issue for their organisation to warrant the expenditure.

Such organisations will need to:

- consider whether it is reasonable for them to adopt practices, procedures and systems to ensure compliance (in view of factors such as the sensitivity of information held and cost); and
- if so – develop and maintain them.

(ii) “Deal with inquiries” about compliance (APP 1(2)(b))

[7.120] The obligation under APP 1(2)(b) to have in place practices, procedures and systems to enable an entity “to deal with inquiries” regarding compliance with the APPs has the *potential* to be significant, including for large organisations with well established privacy regimes. Similar obligations exist under NPP 5 (“Openness”) which requires an organisation to be open and transparent regarding what types of personal information it holds and how it is handled. However, APP 1(2)(b) has a slightly different focus; namely, on enquiries regarding compliance, as opposed to types of information held and how such information is handled.

In effect, APP 1(2)(b) will require organisations to have in place practices and procedures that require staff to respond in an appropriate way to privacy enquiries. Depending on the circumstances, it may, for example, be “reasonable” to “deal with inquiries” by providing customers with a copy of the organisation’s privacy policy (assuming it is sufficiently detailed and accurate to address the issues raised). In other instances, it may require more onerous steps, such as requiring the relevant staff member to refer the enquiry to a manager or Privacy Officer who can provide an informed and considered explanation in response to the specific issues raised.

A type of scenario that APP 1(2)(b) may be seeking to avoid is where, for example, a customer raises a legitimate privacy concern with a customer services officer when completing an application form (eg “Why are you asking for this information?” or “Who will this information be disclosed to?”) and the customer service officer in effect provides a response that avoids or deflects the question (eg “Don’t worry. Information is treated confidentially and we won’t disclose it to anyone”, even though this is not correct, or “There is nothing to be concerned about – we comply with privacy laws.”). Compliance programs that result in responses such as these may not meet APP 1(2)(b) requirements to have systems in place that enable an organisation “to deal with inquiries” regarding privacy compliance as, in this example, the customer’s question will not have been appropriately dealt with.

Privacy policy

- (3) An entity must have a clearly expressed and up-to-date policy (the *privacy policy*) about the management of personal information by the entity.
- (4) Without limiting subsection (3), the privacy policy must contain the following information:
 - (a) the kinds of personal information that the entity collects and holds;
 - (b) how the entity collects and holds personal information;
 - (c) the purposes for which the entity collects, holds, uses and discloses personal information;
 - (d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;
 - (e) how an individual may complain about an interference with the privacy of the individual and how the entity will deal with such a complaint;
 - (f) whether the entity is likely to disclose personal information to overseas recipients;
 - (g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the privacy policy.

SAMPLE ONLY



Pages 1,405-1,424 are not part of this book preview.

[7.380] APP 7—direct marketing

Direct marketing

- (1) If an organisation holds personal information about an individual, the organisation must not use or disclose the information for the purpose of direct marketing unless:
- (a) if the information is sensitive information and paragraph (c) does not apply—the individual has consented to the use or disclosure of the information for that purpose; or
 - (b) if the information is not sensitive information and paragraph (c) does not apply—subsection (2) or (3) applies in relation to the use or disclosure of the information for that purpose; or
 - (c) if:
 - (i) the organisation is a contracted service provider for a Commonwealth contract; and
 - (ii) the organisation collected the information for the purpose of meeting (directly or indirectly) an obligation under the contract;
 the use or disclosure is necessary to meet (directly or indirectly) an obligation under the contract.

Note: An act or practice of an agency may be treated as an act or practice of an organisation.

Personal information collected from the individual

- (2) This subsection applies in relation to the use or disclosure by an organisation of personal information about an individual for the purpose of direct marketing if:
- (a) the organisation collected the information from the individual; and
 - (b) the individual would reasonably expect the organisation to use or disclose the information for that purpose; and
 - (c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and
 - (d) the individual has not made such a request to the organisation.

Personal information collected from another person etc.

- (3) This subsection applies in relation to the use or disclosure by an organisation of personal information about an individual for the purpose of direct marketing if:
- (a) the organisation collected the information from:
 - (i) the individual and the individual would not reasonably expect the organisation to use or disclose the information for that purpose; or
 - (ii) a person other than the individual; and
 - (b) either:
 - (i) the individual has consented to the use or disclosure of the information for that purpose; or
 - (ii) it is impracticable to obtain that consent; and
 - (c) the organisation provides a simple means by which the individual may easily request not to receive direct marketing communications from the organisation; and
 - (d) in each direct marketing communication with the individual:
 - (i) the organisation includes a prominent statement that the individual may make such a request; or
 - (ii) the organisation otherwise draws the individual’s attention to the fact that the individual may make such a request; and
 - (e) the individual has not made such a request to the organisation.

“Direct marketing”

[7.385] APP 7 applies in relation to “direct marketing” activities. The Act does not define the term “direct marketing”, nor has a definition been proposed in the exposure draft legislation.

The Privacy Commissioner has previously advised (see the Commissioner’s *Draft National Privacy Principal Guidelines* (7 May 2001) at p 27) that direct marketing includes:

- an activity promoting the sale or purchase of products or services or promoting charitable fundraising where the individual is approached directly;

- an approach in-person to an individual’s house (eg door-to-door selling);
- an approach by mail, e-mail, telex, facsimile and phone, including an individually targeted approach where an individual is encouraged to buy a service at a distance such as by phone, mail or through a website, or the individual is encouraged to visit a retail and service outlet or to donate to a cause by one of these means; and
- an automated process such as spam e-mail and computer generated voice calls over the phone.

Generally, direct marketing does not include marketing communications via mediums such as radio, newspaper, journals, television and billboards. Accordingly, use and disclosure of personal information for such marketing activities will generally fall outside the scope of APP 7.

Operation (APP 7(1), (2) and (3))

[7.390] APP 7 adopts a complex structure. A detailed overview of how the provision operates is provided below.

APP 7 generally provides that personal information can only be used or disclosed for direct marketing purposes:

- in regards to personal information other than sensitive information (APP 7(1)(b), (2) and (3)) –
 - where the information is collected from the individual concerned – if:
 - such use would be within reasonable expectations; and
 - the organisation provides and abides by an opt-out facility; or
 - where the information is collected from:
 - the individual concerned and such use would *not* be within reasonable expectations; or
 - a third party –
 if:
 - the individual consents *or* it is impractical to obtain consent;
 - the organisation provides and abides by an opt-out facility; and
 - the organisation includes in marketing communications a prominent statement regarding, or otherwise draws the individual’s attention to, the ability to opt-out;
- in regards to sensitive information – where the individual concerned has consented (APP 7(1)(a)); or
- in regards to information collected pursuant to a Commonwealth contract – if such use or disclosure is for the purpose of performing the contract (APP 7(1)(c)).

The requirement to include opt-out facilities closely resembles the requirement under the Spam Act to include unsubscribe facilities. The fact that an opt-out facility is not required in relation to sensitive information (assuming it is not a drafting oversight) appears to be at least partially justified on the basis that consent is required in all circumstances for direct marketing (whereas consent is only required in certain circumstances in relation to non sensitive information).

Comparison with position under NPPs

[7.395] Under NPP 2, personal information can be used and disclosed for direct marketing purposes in a considerably broader set of circumstances than those permitted under APP 7, namely:

- NPP 2.1 – where the information is collected for the purpose of direct marketing;
- NPP 2.1(a) – where such use or disclosure is related (or, in the case of sensitive information, directly related) to the primary purpose of collection and is within reasonable expectations;
- NPP 2.1(b) – where the individual concerned consents;
- NPP 2.1 (c) – where it is impractical to obtain consent before using information for such purposes (certain other requirements must also be met).

In regards to use and disclosure of sensitive information for direct marketing purposes, the NPPs generally don’t – unlike APP 7 – require consent (although consent is generally required to *collect* sensitive information under NPP 10).

Impact (APP 7(1), (2) and (3))

Level of impact: high

[7.400] Relative to NPP 2, APP 7 imposes significant restrictions on the circumstances in which personal information may be used or disclosed for direct marketing purposes. Accordingly, it will have a major impact on the use and disclosure of personal information for direct marketing activities.

(i) Achieving compliance

[7.405] APP 7 adopts a complex structure which results in an equally complex matrix of scenarios. In order to ensure compliance with APP 7, organisations that engage in direct marketing will need to undertake detailed audits of personal information they use and disclose for direct marketing purposes in order to ascertain issues such as:

- what information is used and disclosed for direct marketing purposes?
- is sensitive information used and disclosed for direct marketing purposes?
- the circumstances in which each type of information was collected in order to be able to assess it against the criteria set out under APP 7 (which vary depending on the circumstances) – for example:
 - was the information collected from the individual concerned or a third party?
 - would use or disclosure for direct marketing be within reasonable expectations?
 - would it be impractical to obtain consent?

Further, organisations will need to develop or update systems (including customer relationship management systems and marketing databases) to ensure they are able to manage the complex matrix of compliance requirements.

(ii) Opt-out facilities

[7.410] The requirement to include opt-out facilities will provide individuals with a right not currently enjoyed under the NPPs. Generally, under the NPPs (as opposed to, for example, the Spam Act), an organisation is permitted to continue to send direct marketing communications even if an individual requests not to receive them (although it would, of course, constitute poor business practices not to comply with the individual's request).

(iii) Consent

[7.415] In view of the significantly broader set of circumstances in which consent must be present to use and disclose personal information for direct marketing purposes, organisations will need to consider obtaining consent to use and disclose information for marketing purposes at the time of collection, either through standard terms of service/sale or consent forms.

In view of practical difficulties associated with distinguishing between customers from whom consent is required, and those from whom it is not, it may often be preferable to collect consents from *all* customers.

In regards to obtaining consent, consent is defined under the Privacy Act to mean express or implied consent (and this definition will remain). Accordingly, an organisation will not *necessarily* need to obtain express written consent (although, this is always preferable) as it may be able to conclude that consent was implied by virtue of, for example, the circumstances in which the information concerned was collected.

Individual may request not to receive direct marketing communications etc.

- (4) If an organisation uses or discloses personal information about an individual for the purpose of direct marketing by the organisation, or for the purpose of facilitating direct marketing by other organisations, the individual may:
- (a) if the organisation uses or discloses the information for the purpose of direct marketing by the organisation—request not to receive direct marketing communications from the organisation; and
 - (b) if the organisation uses or discloses the information for the purpose of facilitating direct marketing by other organisations—request the organisation not to use or disclose the

SAMPLE ONLY



Pages 1,428-1,462 are not part of this book preview.

Annotated Draft Australian Privacy Principles

PUBLIC SECTOR ANNOTATIONS

[7.700] APP 1—open and transparent management of personal information

(1) The object of this principle is to ensure that entities manage personal information in an open and transparent way.

Compliance with the Australian Privacy Principles etc.

(2) An entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions and activities that:

- (a) will ensure that the entity complies with the Australian Privacy Principles; and
- (b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the Australian Privacy Principles.

Purpose (APP 1(2))

[7.705] The Government's *Companion Guide – Australian Privacy Principles* (June 2010) outlines the purpose of APP 1 as follows (at 9):

The requirement for open and transparent management is the first of the Australian Privacy Principles because it will emphasise that entities should first plan *how* they will handle personal information before they collect and process it.

The principle is also intended to outline that part of complying with the Australian Privacy Principles is making sure that entities consider their privacy obligations when planning new systems.

This is part of international moves towards a “privacy by design” approach, that is, ensuring that privacy and data protection compliance is included in the design of information systems from their inception. (emphasis in original)

Accordingly, APP 1(2) aims to ensure that entities take a *proactive* approach to privacy compliance (ie foreseeing privacy risks and putting systems in place to avoid such risks eventuating), rather than a *reactive* one (eg resolving privacy issues and complaints as they arise, resulting in privacy policies and procedures being developed piecemeal).

Equivalent IPPs

[7.710] Obligations under APP 1(2) have no express equivalent under the IPPs (although such obligations are, to a large extent, implicit).

Impact of changes (APP 1(2))

Level of impact: medium

(i) Measures to ensure compliance (APP 1(2)(a))

[7.715] Whilst the IPPs do not expressly require an agency to take reasonable steps to implement practices, procedures and systems to ensure compliance, it has nevertheless been a practical reality for many agencies that such measures need to be taken as part of risk management programs to comply with the Act. For such agencies, APP 1(2) will have little impact as it is merely formalising a practical requirement that already exists under the IPPs.

However, APP 1(2) does have ramifications for agencies that have *not* adopted practices, procedures and systems to ensure compliance where it would be *reasonable* for them to do so. Entities that may fall within this category could, for example, include a small agency which has not formalised its information handling procedures by developing relevant policies and internal guidelines, which deals with sensitive issues and which considers privacy matters are partially or largely covered by other laws or governance mechanisms impacting on information handling practices (eg duties of confidence and records management laws).

Such an agency will need to:

- consider whether it is reasonable for it to adopt practices, procedures and systems to ensure compliance (in view of factors such as the sensitivity of information held and cost); and
- if so – develop and maintain them.

(ii) “Deal with inquiries” about compliance (APP 1(2)(b))

[7.720] The obligation to have in place practices, procedures and systems to enable an agency to deal with enquiries regarding compliance with the APPs has the potential to be significant, including for large agencies with well established privacy compliance programs. Similar obligations exist under IPP 5 (“Information relating to records kept by record-keeper”) which require agencies to be open and transparent regarding what types of personal information they hold and how it is handled. However, APP 1(2)(b) has a different focus; namely, on enquiries regarding compliance, as opposed to types of information held and how such information is handled.

In effect, APP 1(2)(b) will require agencies to have in place practices and procedures that require staff to respond in an appropriate way to privacy enquiries. Depending on the circumstances, it may be “reasonable” to “deal with inquiries” by providing individuals with a copy of the agency’s privacy policy (assuming it is sufficiently detailed and accurate to address the issues raised). In other instances, it may require more onerous steps, such as requiring the relevant staff member to refer the enquiry to a manager or Privacy Contact Officer who can provide an informed and considered explanation in response to the specific issues raised.

A type of scenario that APP 1(2)(b) may be seeking to avoid is where an individual raises a privacy concern, for example, with a client services officer when completing an application form (eg “Why are you asking for this information?” or “Who will this information be disclosed to?”) and the client services officer in effect provides a response that avoids or deflects the question (eg “Don’t worry. Information is treated confidentially and we won’t disclose it to anyone”, even though this is not correct, or “There is nothing to be concerned about – we are bound by the Privacy Act.”). Policies and procedures that result in responses such as these would not appear to meet APP 1(2)(b) requirements to have systems in place to enable the agency “to deal with inquiries or complaints”.

Privacy policy

- (3) An entity must have a clearly expressed and up-to-date policy (the *privacy policy*) about the management of personal information by the entity.
- (4) Without limiting subsection (3), the privacy policy must contain the following information:
 - (a) the kinds of personal information that the entity collects and holds;
 - (b) how the entity collects and holds personal information;
 - (c) the purposes for which the entity collects, holds, uses and discloses personal information;
 - (d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;
 - (e) how an individual may complain about an interference with the privacy of the individual and how the entity will deal with such a complaint;
 - (f) whether the entity is likely to disclose personal information to overseas recipients;
 - (g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located if it is practicable to specify those countries in the privacy policy.

Equivalent IPPs (APP 1(3) and (4))

[7.725] APP 1(3) reflects obligations under IPP 5.3 to maintain what has become known as Personal Information Digests. However, APP 1(3) refers to the document as a “privacy policy” and specifies different types of information that must be contained in the document. Obligations under IPP 5.3 and 5.4 regarding requirements to prepare, maintain and make available Personal Information Digests have, in effect, been replaced by the obligation to maintain a privacy policy.

SAMPLE ONLY



Pages 1,465-1,468 are not part of this book preview.

However, APP 3(5) will have a significant impact as it introduces a new set of obligations on agencies in regards to collections from third parties. In effect, APP 3(5) prohibits a collection from a third party unless one of the exceptions under APP 3(5)(a) or (b) apply.

Agencies commonly collect personal information about individuals from a large number of third parties – for example, other agencies, family members, medical practitioners and businesses. Agencies will need to review all such collections and assess whether they meet the requirements of either APP 3(5)(a) or (b). If not, the agency will need to cease those types of collections and develop policies, procedures and systems to ensure that such information is only collected directly from the individuals concerned.

Solicited personal information

(6) This principle applies to the collection of personal information that is solicited by an entity.

“Solicited”

[7.840] Proposed s 15 defines “solicits” as follows:

an entity solicits personal information if the entity requests a person to provide the personal information, or to provide a kind of information in which that personal information is included.

As such, information will likely be solicited if an agency asks for:

- specific information – such as on a form requesting name and DOB; or
- broad categories of information – such as:
 - an application form requesting reasons as to why an individual believes a decision that has been made is unfair; or
 - an online form seeking feedback about services provided.

Solicited information will not, for example, include information contained in a letter from a member of the public providing a confidential tip-off about suspected fraud where the agency has not requested such information and has no statutory responsibilities or functions to investigate such frauds.

Scope of APP 3 – solicited collections only

[7.845] APP 3(6) limits the application of APP 3 to solicited collections of personal information (although, in the absence of the word “only” before “applies”, it could be interpreted as being intended to clarify that APP 3 applies to solicited collections *in addition to* unsolicited collections). Accordingly, APP 3 does not apply in relation to collections of unsolicited personal information (including unsolicited sensitive information) – such collections are regulated under APP 4.

[7.865] APP 4—receiving unsolicited personal information

- (1) If:
 - (a) an entity receives personal information about an individual; and
 - (b) the entity did not solicit the information;
 the entity must, within a reasonable period of receiving the information, determine whether or not the entity could have collected the information under Australian Privacy Principle 3 if the entity had solicited the information.
- (2) The entity may use or disclose the personal information for the purposes of making the determination under subsection (1).
- (3) If the entity determines that the entity could have collected the personal information, Australian Privacy Principles 5 to 13 apply in relation to the information as if the entity had so collected the information.
- (4) If the entity determines that the entity could not have collected the personal information, the entity must, as soon as practicable but only if it is lawful and reasonable to do so:
 - (a) destroy the information; or
 - (b) ensure that the information is no longer personal information.

Equivalent IPPs

[7.870] The IPPs do not have equivalent provisions to APP 4.

IPP 2 (regarding privacy notices at the time of collection) and IPP 3 (requiring that information be relevant to the collection purpose, up-to-date, complete and not collected in an unreasonably intrusive way) apply only to *solicited* collections – they do not apply to *unsolicited* collections.

IPP 1 (which requires information to be necessary for a function or activity and collected fairly and lawfully) makes no distinction between solicited and unsolicited collections and, as such, is generally understood to apply to both. In the context of the private sector NPPs, it is well established that a collection of unsolicited personal information is a collection of personal information for the purposes of the Act (see, eg, *M v Financial Institution* [2009] PrivCmrA 16 and *E v Private School* [2010] PrivCmrA 6). There is nothing to suggest the position is any different under IPP 1. Accordingly, an agency is, for example, required to ensure that a collection of unsolicited information is necessary for a function or activity under IPP 1.1. In this regard, IPP 1 is similar to APP 4(1) (ie an agency is required to assess whether the unsolicited collection is permitted against the general criteria for collections under IPP 1.1).

Operation (APP 4)

[7.875] APP 4 requires an agency that receives unsolicited personal information to consider whether it would have been permitted to collect the information under APP 3 if it had solicited the information.

In particular, it must ensure that:

- if the information is not sensitive information – the information is reasonably necessary for, or directly related to, one or more of the agency’s functions or activities (APP 3(1)); or
- if the information is sensitive information (APP 3(2)) –
 - both of the following apply:
 - the information is reasonably necessary for, or directly related to, one or more of the agency’s functions or activities; and
 - the individual consents to the collection of the information; or
 - one of the exceptions under APP 3(3) applies to the information.

If the collection would not be permitted under APP 3, the agency must generally destroy or de-identify the information, unless it is unlawful or unreasonable to do so.

Interaction with *Archives Act 1983* (Cth)

[7.880] The obligation for agencies to destroy information is a significant one in view of obligations under s 24 of the *Archives Act 1983* not to destroy a Commonwealth record (within the meaning of that Act) unless, among other things, required to do so by law. If an agency is considering destroying all information in a record and, hence, destroying the record itself, the agency must ensure this is permitted under the *Archives Act* (see, for example, the Australian Government Management Advisory Committee’s *Note for File: A Report on Recordkeeping in the Australian Public Service* (2007) which provides guidance on when Commonwealth records, including low-value documents, can be destroyed).

Impact of changes (APP 4)

Level of impact: high

[7.885] Agencies will be under significant new obligations in regards to collections of unsolicited information by virtue of the fact that obligations under APP 4 that are equivalent to those under IPPs 2 and 3 (which only apply to solicited collections) apply to both solicited *and* unsolicited collections.

For example:

- An agency currently has no notification obligations under IPP 2 in regards to collections of unsolicited personal information. An agency will now have notification obligations under APP 5 in regards to such collections.
- Agencies are often in receipt of unsolicited sensitive information about third parties (eg a letter reporting suspected fraud by a person providing details about the person’s criminal record). In regards to such collections, agencies will now need to assess whether the information could have

SAMPLE ONLY



Pages 1,481-1,550 are not part of this book preview.

[11.460] 10 Limits on use of health information

- (1) An organisation that holds health information must not use the information for a purpose (a *secondary purpose*) other than the purpose (the *primary purpose*) for which it was collected unless:
- (a) **Consent**
the individual to whom the information relates has consented to the use of the information for that secondary purpose, or
 - (b) **Direct relation**
the secondary purpose is directly related to the primary purpose and the individual would reasonably expect the organisation to use the information for the secondary purpose, or
Note. For example, if information is collected in order to provide a health service to the individual, the use of the information to provide a further health service to the individual is a secondary purpose directly related to the primary purpose.
 - (c) **Serious threat to health or welfare**
the use of the information for the secondary purpose is reasonably believed by the organisation to be necessary to lessen or prevent:
 - (i) a serious and imminent threat to the life, health or safety of the individual or another person, or
 - (ii) a serious threat to public health or public safety, or
 - (d) **Management of health services**
the use of the information for the secondary purpose is reasonably necessary for the funding, management, planning or evaluation of health services and:
 - (i) either:
 - (A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or
 - (B) reasonable steps are taken to de-identify the information, and
 - (ii) if the information is in a form that could reasonably be expected to identify individuals, the information is not published in a generally available publication, and
 - (iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or
 - (e) **Training**
the use of the information for the secondary purpose is reasonably necessary for the training of employees of the organisation or persons working with the organisation and:
 - (i) either:
 - (A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or
 - (B) reasonable steps are taken to de-identify the information, and
 - (ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and
 - (iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or
 - (f) **Research**
the use of the information for the secondary purpose is reasonably necessary for research, or the compilation or analysis of statistics, in the public interest and:
 - (i) either:
 - (A) that purpose cannot be served by the use of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained and it is impracticable for the organisation to seek the consent of the individual for the use, or
 - (B) reasonable steps are taken to de-identify the information, and

- (ii) if the information could reasonably be expected to identify individuals, the information is not published in a generally available publication, and
 - (iii) the use of the information is in accordance with guidelines, if any, issued by the Privacy Commissioner for the purposes of this paragraph, or
 - (g) **Find missing person**
the use of the information for the secondary purpose is by a law enforcement agency (or such other person or organisation as may be prescribed by the regulations) for the purposes of ascertaining the whereabouts of an individual who has been reported to a police officer as a missing person, or
 - (h) Suspected unlawful activity, unsatisfactory professional conduct or breach of discipline the organisation:
 - (i) has reasonable grounds to suspect that:
 - (A) unlawful activity has been or may be engaged in, or
 - (B) a person has or may have engaged in conduct that may be unsatisfactory professional conduct or professional misconduct under the *Health Practitioner Regulation National Law (NSW)*, or
 - (C) an employee of the organisation has or may have engaged in conduct that may be grounds for disciplinary action, and
 - (ii) uses the health information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities, or
 - (i) **Law enforcement**
the use of the information for the secondary purpose is reasonably necessary for the exercise of law enforcement functions by law enforcement agencies in circumstances where there are reasonable grounds to believe that an offence may have been, or may be, committed, or
 - (j) **Investigative agencies**
the use of the information for the secondary purpose is reasonably necessary for the exercise of complaint handling functions or investigative functions by investigative agencies, or
 - (k) **Prescribed circumstances**
the use of the information for the secondary purpose is in the circumstances prescribed by the regulations for the purposes of this paragraph.
- (2) An organisation is not required to comply with a provision of this clause if:
- (a) the organisation is lawfully authorised or required not to comply with the provision concerned, or
 - (b) non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including the *State Records Act 1998*).
- (3) The Ombudsman’s Office, Health Care Complaints Commission, Anti-Discrimination Board and Community Services Commission are not required to comply with a provision of this clause in relation to their complaint handling functions and their investigative, review and reporting functions.
- (4) Nothing in this clause prevents or restricts the disclosure of health information by a public sector agency:
- (a) to another public sector agency under the administration of the same Minister if the disclosure is for the purposes of informing that Minister about any matter within that administration, or
 - (b) to any public sector agency under the administration of the Premier, if the disclosure is for the purposes of informing the Premier about any matter.
- (5) The exemption provided by subclause (1) (j) extends to any public sector agency, or public sector official, who is investigating or otherwise handling a complaint or other matter that could be referred or made to an investigative agency, or that has been referred from or made by an investigative agency.

Equivalent/concurrent obligations under NPPs

[11.465] In relation to the use of information under the Privacy Act, see NPP 2 under [3.260].

Related commentary

[11.470] Commentary on the following related issues appears where indicated:

- meaning of primary purpose of collection – at [3.280];
- obtaining consent – at [133.45];
- uses that are required or authorised by law – at [3.685];
- “directly related” uses – at [3.455].

Directly related uses within reasonable expectations (HPP 10(1)(b))

[11.475] Privacy NSW’s *Statutory guidelines on the management of health services* indicate (at p 5) that examples of directly related uses within reasonable expectations that may fall within the ambit of the exemption under HPP 10(1)(b) include:

- providing ongoing care to patients;
- investigating and managing adverse incidents or complaints about care or patient safety;
- quality assurance activities such as monitoring, evaluating or auditing the provision of a relevant product or service;
- managing the provision of a service or product;
- following up complaints;
- recalling products;
- administrative activities associated with providing, following up on or receiving payment;
- sending reminders to regular patients; and
- managing a legal claim.

The *Statutory guidelines on training* indicate (at p 5) that: (a) use of a patient’s file for training a receptionist might fall within the exemption, provided only information that is necessary for the training is used; and (b) where a person has been informed that their information will be used for training as part of an admission procedure, this would generally be considered a directly related secondary purpose within reasonable expectations. The *Statutory guidelines on research* indicate that, whilst it is unlikely that many research activities will fall within the exemption, some compilation or analysis of statistics activities may do so, eg compiling statistics about the number of patients treated for a particular disease (at p 5).

The Victorian Health Services Commissioner has held under a similar provision of the *Health Records Act 2001* (Vic) that disclosure of a client list by a fitness centre to a supplier that used the list for direct marketing purposes and paid the fitness centre a commission from sales was not within reasonable expectations (*Private Lives: Your Guide to Privacy Law in Victoria* (Privacy Victoria, 2003)).

Training guidelines (HPP 10(1)(e))

[11.480] Privacy NSW has issued *Statutory guidelines on training* for the purposes of HPP 10(1)(e) which set out requirements when relying on the training exemption. In addition, the guidelines indicate that:

- in determining whether a use is “reasonably necessary”, regard should be had to what degree the information is needed for the training, eg hypothetical information may be sufficient (at p 7);
- “training” means any course, instruction or work experience offered by, or in connection with, an organisation for the purpose of teaching or education, eg an induction or orientation course for new employees, grand rounds, observing the provision of health services or an educational case conference (at p 7);
- the training exemption applies to the training of employees as well as non-employees who are working with the organisation (eg persons working on commission, local or foreign students in medicine, nursing and other related health professions on clinical practice placements) but does not apply to persons who are not working with the organisation (at pp 7-8);
- de-identified information should be used wherever possible, which may require identified information to first be de-identified. However, this will not always be appropriate, eg during

SAMPLE ONLY



Pages 1,554-1,700 are not part of this book preview.

[14]

Privacy Act 1988 (Cth) – Coverage

Entities to which Act applies.....	[14.10]
Overview	[14.10]
IPPs and NPPs	[14.15]
Public sector “agencies”	[14.20]
Private sector “organisations”	[14.25]
Meaning of “organisation”	[14.25]
Non organisations treated as organisations	[14.30]
Exempt entities.....	[14.40]
Public sector	[14.45]
Private sector	[14.50]
Entities excluded from being an organisation	[14.50]
Meaning of “small business operator”	[14.55]
Certain entities excluded	[14.60]
Acts in personal or non business capacity	[14.65]
Health service providers.....	[14.70]
Annual Turnover	[14.75]
Acts and practices to which Act applies.....	[14.85]
Meaning of “act or practice”	[14.85]
Overseas acts and practices.....	[14.90]
Must be link with Australia.....	[14.95]
Carrying on business in Australia	[14.100]
Prescribed acts and practices by small business operators	[14.105]
Exempt acts and practices – public sector	[14.115]
Exempt acts and practices – private sector	[14.125]
Personal, family and household affairs	[14.130]
Individual acting in non business capacity.....	[14.135]
Employee records	[14.140]
Definition of employee records.....	[14.145]
Limitations on exemption	[14.150]
Application in relation to directors and other company officers	[14.155]
Cases.....	[14.155]
Related bodies corporate.....	[14.160]
“Related body corporate”	[14.165]
Primary purpose of collection remains the same.....	[14.170]
Does not apply to sensitive information.....	[14.175]
Changes in partnership.....	[14.180]
Journalism.....	[14.185]
Definition of media organisation	[14.190]
Cases.....	[14.190]
Political acts and practices	[14.195]
Political representatives	[14.200]
Contractors and sub contractors for political representatives.....	[14.205]
Volunteers for registered political parties	[14.210]
Cases.....	[14.210]
Contracted service providers for governments	[14.215]
Required by foreign law	[14.220]
Other	[14.225]

Information to which Act applies.....	[14.235]
Personal information	[14.240]
Sensitive information	[14.245]
Health information	[14.250]
Cases	[14.250]
Must be held in a record	[14.255]
Definition of “record”	[14.260]
Generally available publications	[14.265]
Information collected pre NPPs	[14.275]
Relevant collection dates	[14.275]
NPPs 1, 3 (re collection) and 10	[14.280]
Cases.....	[14.280]
NPP 2	[14.285]
Cases.....	[14.285]
NPPs 3 (re uses and disclosures), 4, 5, 7 and 9.....	[14.290]
Cases.....	[14.290]
NPP 6	[14.295]
Cases.....	[14.295]
NPP 8	[14.300]
Delayed commencement for small businesses	[14.305]

SAMPLE ONLY



Pages 1,703-1,719 are not part of this book preview.

Employee records

Publications, guidelines and related materials

- Commentary on job applicants and recruitment at [144]

[14.140] In regards to private sector organisations, the Privacy Act does not apply to an act or practice engaged in by an organisation that is, or was, an employer of an individual and that is directly related to a current or former employment relationship between the employer and the individual and an employee record held by the organisation relating to the individual (s 7B(3)). There is no equivalent exemption for public sector agencies.

The term “directly related” is not defined by the Act. The Privacy Commissioner has advised, by way of example, that the disclosure of information during due diligence about employees to a purchaser would generally be considered to be directly related to the employment relationship and permitted under the exemption (*Information Sheet 16 – Application of Key NPPs to Due Diligence and Completion When Buying and Selling a Business*).

The employee records exemption applies only to private sector organisations. The exemption does not apply in relation to public sector agencies.

At the time that the exemption was established (with the passing of the private sector provisions in 2000), the Attorney-General indicated that the purpose of the exemption was to enable privacy protection of employee records to be dealt with under workplace relations legislation (see Attorney-General, *Fact Sheet on Privacy in the Private Sector – Employee Records* (22 December 2000)). However, the gap was never filled, with such legislation continuing to provide only limited protection solely in relation to a narrow class of employee records.

Definition of employee records

[14.145] The Act provides a broad definition of “employee record”. It provides (s 6(1)):

employee record, in relation to an employee, means a record of personal information relating to the employment of the employee. Examples of personal information relating to the employment of the employee are health information about the employee and personal information about all or any of the following:

- (a) the engagement, training, disciplining or resignation of the employee;
- (b) the termination of the employment of the employee;
- (c) the terms and conditions of employment of the employee;
- (d) the employee’s personal and emergency contact details;
- (e) the employee’s performance or conduct;
- (f) the employee’s hours of employment;
- (g) the employee’s salary or wages;
- (h) the employee’s membership of a professional or trade association;
- (i) the employee’s trade union membership;
- (j) the employee’s recreation, long service, sick, personal, maternity, paternity or other leave;
- (k) the employee’s taxation, banking or superannuation affairs.

The employee record exemption does not apply to information held about job applicants that have never become employees of the organisation as the requisite former or current employment relationship does not exist. However, the exemption does apply to personal information held about an employee relating to when they were an applicant as that information became part of their employee record when they were employed (Privacy Commissioner, *Information Sheet 12 – Coverage of and Exemptions from the Private Sector Provisions* (OPC, 2001) at p 3 and *Guidelines on Privacy in the Private Health Sector* (OPC, 2001) at p vii).

Limitations on exemption

[14.150] It is evident from the wording of the definition of an employee record that, if information that is not “directly related” to the employment relationship is recorded in the employee record, that information does not fall within the exemption.

For example, if information relating to the employee’s attendance at the workplace in a personal capacity, such as a gym receptionist attending the gym in his or her leisure time, is recorded in his or her employee record, that information is not, in the absence of special circumstances, subject to the exemption. An example of special circumstances might be where the employee's attendance at the workplace is part of his or her work agreement, such as an entitlement to attend the gym free of charge, in which case the information does relate to their employment and will be subject to the exemption.

Similarly, as the employee record exemption applies to an act or practice by an employer that is directly related to an employment relationship, a use or disclosure of information contained within an employee record that is not directly related to the employment relationship will not fall within the exemption. The exemption is unlikely to include, for example, a disclosure of employee information by an employer to a marketing company for the purpose of enabling the marketing company to send marketing communications to the employee about products that are unrelated to the employee’s work.

As the employee records exemption only applies to an act or practice engaged in by an employer, an organisation receiving an employee record from the employer, such as a superannuation company or a contractor, cannot rely on the exemption as it will not enter into an employment relationship with the relevant employee. Accordingly, the recipient organisation will be obliged to handle the information in accordance with the NPPs.

Application in relation to directors and other company officers

[14.155] Personal information collected about company officers, such as directors and company secretaries, who are paid fees for their services, generally will not be subject to the employee records exemption as such officers generally are not employees. However, purposes for which such information is generally used and disclosed will, depending on the circumstances, often be permitted under the NPPs, either on the basis that it is for the primary purpose of collection (NPP 2.1), a related purpose within reasonable expectations (NPP 2.1(a)) or with consent (NPP 2.1(b)).

Personal information about executives engaged on an employee basis will be subject to the employee records exemption.

Cases

- ***N v Commonwealth Agency [2009] PrivCmrA 17:*** Disclosure by an employer of an employee’s personnel and related files to a contractor to enable the contractor to investigate the handling of complaints made by the employee were held to be directly related to the employment relationship.
- ***C v Commonwealth Agency [2005] PrivCmrA 3:*** C and his wife were employees of a Commonwealth agency (the agency engaged in commercial activities and, to that extent, was bound by the NPPs, rather than the IPPs, pursuant to s 7A(3)). C's wife had commenced proceedings against the agency for compensation in which the wife claimed that she was unable to afford certain expenses. The agency obtained information about C's income from its payroll department and submitted it to its legal counsel as evidence of the wife's financial position. *Outcome:* Whilst the personal information relating to C was an employee record, the act of disclosing it to legal counsel in relation to proceedings involving C's wife was not directly related to C's employment and, as such, did not fall within the employee records exemption (the disclosure was, however, permitted on other grounds).
- ***B v Cleaning Company [2009] PrivCmrA 2:*** C was employed by a large cleaning company (E) for several years before resigning. C owed money to a third party (TP) and defaulted on payment. TP contacted E asking for information to assist in locating C. E disclosed C's personal information to TP, including their address and financial details which were contained in C's employee record. E claimed that the disclosure was subject to the employment records exemption and, as such, they

SAMPLE ONLY



Pages 1,722-1,950 are not part of this book preview.

[21]

Investigations by Commissioner

Introduction	[21.10]
Commissioner’s approach.....	[21.20]
Education	[21.25]
Conciliation	[21.30]
Determinations.....	[21.35]
Types of investigations	[21.45]
Complaint	[21.50]
Own motion	[21.55]
Grounds on which complaints may be rejected	[21.65]
Grounds	[21.65]
When is a matter “adequately dealt with”?	[21.67]
Investigation procedures	[21.75]
Evidence.....	[21.85]
Commissioner’s information gathering and other powers.....	[21.95]
Determinations.....	[21.105]
Introduction	[21.105]
When will Commissioner consider making a determination?	[21.110]
Dismissal of complaint	[21.115]
Declaration of interference with privacy and to cease conduct.....	[21.120]
Declaration that should perform act or course of conduct	[21.125]
Declaration that entitled to compensation.....	[21.130]
Assessment of compensation	[21.135]
Cases.....	[21.140]
Declaration that inappropriate to take further action	[21.145]
Declaration as to costs	[21.150]
Order to vary or attach information	[21.155]
Review of determinations	[21.160]
Enforcement of determinations.....	[21.165]

SAMPLE ONLY



Pages 1,952-1,953 are not part of this book preview.

or by an organisation self-reporting an incident to the Commissioner's office. The Commissioner's office has opened 59 own-motion investigations in the year up to August 2011 ("Thousands of privacy breaches going unreported", *The Sydney Morning Herald*, 27 July 2011).

A significant limitation on the Commissioner's powers in relation to own-motion investigations is that he or she does not have the power to impose a sanction on an organisation following such an investigation, even where a breach is found to have occurred. In view of this, the Commissioner has accepted written undertakings by respondent organisations to own-motion investigations. In July 2010, the Commissioner concluded an own-motion investigation into Google's collection of unsecured WiFi payload data in Australia using "Street View" vehicles. The Commissioner found that, on the information available, she was satisfied that any collection of personal information would have breached the Privacy Act. The Commissioner accepted a written undertaking from Google that it would:

- publish an apology to Australians in Google's official Australian blog for its collection of unsecured WiFi 'payload' data;
- undertake to conduct a privacy impact assessment (PIA) on any new Street View data collection activities in Australia that include personal information;
- provide a copy of the PIAs to the Commissioner; and
- regularly consult with the Commissioner about personal data collection activities arising from significant product launches in Australia.

Grounds on which complaints may be rejected

Grounds

[21.65] The Privacy Commissioner may refuse to investigate, or discontinue investigating, a complaint on various grounds (s 41(1)), and often elects to do so where, for example, a complaint is unsubstantiated or an organisation has dealt appropriately with a complaint. The specific grounds on which the Commissioner may, or must, refuse to investigate or discontinue an investigation are:

- The individual has not first complained to the organisation, unless the Privacy Commissioner considers that it is not appropriate for the complainant to do so (s 40(1A));
- There has not been an "interference with the privacy" of an individual (as defined in ss 13 and 13A) (s 41(1)(a)) – This will be the case if, for example, a respondent entity is not bound by the Act, ie it is not an "organisation" or an "agency" within the meaning of the Act;
- The complaint was made more than 12 months after the complainant became aware of the act or practice to which it relates (s 41(1)(c)).
- The complaint is frivolous, vexatious, misconceived or lacking in substance (s 41(1)(d)).

In *P v Various Entities* [2003] PrivCmrA 14, the Privacy Commissioner exercised his discretion to decline to investigate a complaint. In that case, the complainant complained about various medical treatments provided to him and the way the media and other professional bodies had been dealing with him. The relevant facts were unclear and the respondents were unknown, even after telephone discussions were held with the complainant. The Commissioner declined to investigate the complaint on the grounds that it was lacking in substance since it was unclear who had allegedly misused the complainant's personal information.

- The complaint has been, or is being, dealt with adequately as a result of an application under another law (s 41(1)(e)) – This may apply where, for example, a complaint relating to the same incident may be lodged with a health services commissioner pursuant to a health records statute
- Another law provides a more appropriate remedy for the complaint (s 41(1)(f)).
- The individual has complained to the relevant organisation which has either dealt, or is dealing, with the complaint appropriately or it has not yet had adequate opportunity to deal with it (s 41(2)) – see the commentary at [21.67].
- Where certain offences may have been committed (including a tax file number offence, healthcare identifier offence, anti-money laundering and counter-terrorism financing offence or credit reporting offence) (s 49).

Further, the Commissioner may:

- refer complaints in certain circumstances to other authorities, including the Australian Human Rights Commission and the Commonwealth Ombudsman (see s 50);
- defer an investigation in circumstances relating to where the respondent has applied for a public interest determination relating to the relevant conduct (s 41(3));
- suspend investigating a matter that is being investigated by the Auditor-General (s 51).

When is a matter “adequately dealt with”?

[21.67] The Privacy Commissioner often refuses to investigate a complaint on the basis that the respondent has either dealt, or is dealing, with the complaint appropriately (pursuant to s 41(2)), emphasising the importance for entities of seeking to resolve complaints directly with individuals before they are escalated to the Commissioner’s office. If an entity has offered to take reasonable remedial action in settlement of a complaint and the complainant has rejected this offer, the Commissioner will often refuse to investigate further on this basis.

The Privacy Commissioner’s *Privacy complaints: practice and procedure manual* provides guidance on the considerations the Commissioner will take into account when assessing whether to discontinue an investigation on the basis that the respondent has adequately dealt with the complaint:

If the respondent makes what we consider to be an appropriate offer we may decide that we will cease the investigation under s 41(2)(a) on the grounds that the respondent has dealt adequately with the matter. However ... significant caution should be exercised when closing a complaint as adequately dealt with where the complainant has expressed that they are not satisfied with the outcome.

Generally, it will only be appropriate to decide to close a complaint in these circumstances where the respondent has taken steps to address the complaint which are commensurate with resolutions achieved in similar complaints, and the complainant is highly unlikely to achieve a better resolution if the complaint were to go to determination.

In *A v Insurer* [2002] PrivCmrA 1, the complainant alleged that NPP 1.3 information regarding an insurance organisation’s uses and disclosures was deficient as it was only provided at the time of making a claim (rather than at the time of concluding the contract) and merely stated information would be disclosed (among other entities) to “consultants”. Once the organisation had agreed to provide the relevant NPP 1.3 information at the time of contracting, reword its privacy policy to specify more clearly whom information would be disclosed to, include a definition of “consultant” on its website (although not in its policy) and make the definition available upon request, it was held that the respondent had adequately dealt with the matter.

Similarly, in *B v Private Health Insurer* [2002] PrivCmrA 2, a health insurance fund that erroneously disclosed a person’s sensitive information to employers in a sample form was held to have adequately dealt with the matter by revising and strengthening its checking procedures to reduce the risk of recurrence, providing further staff training, advising all recipients to destroy the information, taking disciplinary action against the staff member responsible and reminding staff that breaching customers’ privacy may lead to disciplinary consequences.

Investigation procedures

[21.75] Investigations are generally conducted informally by the Privacy Commissioner’s office. Often, investigations will be conducted solely by written, and sometimes also telephone, correspondence with each of the parties. Throughout the correspondence process, the Commissioner will generally seek relevant information from the respondent, form a preliminary conclusion as to whether a breach occurred, seek the respondent’s response to the preliminary conclusion, form a final conclusion as to whether there was a breach and, if so, seek to negotiate a settlement between the parties. In certain circumstances, staff from the Commissioner’s office may attend the respondent’s premises, particularly where, for example, a complaint relates to a new technology and the Commissioner’s office wishes to learn more about data management practices surrounding the technology.

The Privacy Act provides that an investigation must be conducted in private but otherwise in a manner that the Privacy Commissioner thinks fit (s 43(2)).

SAMPLE ONLY



Pages 1,956-2,640 are not part of this book preview.

[45]

Contracted service providers (public sector)

Introduction	[45.10]
What is a contracted service provider?.....	[45.20]
Commonwealth agency contracts	[45.30]
Mandatory privacy terms	[45.30]
Drafting terms	[45.35]
Disclosures to contractors	[45.40]
Contractors that are small businesses.....	[45.45]
Contractor obligations under NPPs.....	[45.50]
Conflict between IPPs and NPPs.....	[45.50]
Matters not covered by IPPs.....	[45.55]
Prohibition on use of information for direct marketing	[45.60]
State and Territory government contracts	[45.70]

Publications, guidelines and related materials

- Australian Government Solicitor, *Legal Briefing (No 63) – Outsourcing: Agency Obligations under the Privacy Act (2002)*
- OPC, *Private Sector Information Sheet 14 – 2001 Privacy Obligations for Commonwealth Contracts*
- OICQ, *Privacy Guideline – Contracted service providers*
- Commentary on contractors at [138]

Introduction

[45.10] The Privacy Act contains special provisions concerning contracted service providers for government agencies. The need for such provisions arises largely due to the fact that contractors:

- are usually private sector entities that are not bound by privacy laws that apply to public sector agencies;
- if they are bound by the Privacy Act – are bound by the private sector NPPs;
- if they are not bound by the Privacy Act (eg a small businesses) – are under no legal obligation under the Act to handle personal information appropriately.

In regards to Commonwealth agency contracts, the provisions generally provide that a contractor:

- is to be contractually bound by the agency to comply with the IPPs;
- is bound by the NPPs to the extent that the IPPs have no equivalent; and
- can do an act that is inconsistent with the NPPs if permitted by the contract.

For commentary on practical issues relating to dealing with contractors, see [138].

What is a contracted service provider?

[45.20] A contracted service provider, for a government contract, means (s 6(1)):

- an organisation that is or was a party to the contract and that is or was responsible for the provision of services to a Commonwealth agency or a State or Territory authority under the contract (including services to third parties in connection with the performance of the functions of the agency (s 6(9)); or
- a subcontractor for the contract.

Due to the inclusion of the words "or was" in the definition of a contracted service provider, a contractor's obligations under the Act continue after the completion of the contract.

In regards to Commonwealth contracts, where the contracted service provider is a State or Territory authority (eg where a State authority provides research services for a Commonwealth agency), the State or Territory authority is not a "contracted service provider" within the meaning of the Act as such authorities are excluded from the meaning of the term by virtue of their exclusion from the meaning of an "organisation" (see ss 6(1) and 6C) – only an "organisation" can be a contracted service provider. The authority will generally be bound by applicable State or Territory privacy laws or administrative directions. However, a Commonwealth agency should still take appropriate contractual measures with such an authority to ensure appropriate privacy protections for personal information that will be handled by the authority.

Commonwealth agency contracts

Mandatory privacy terms

[45.30] Section 95B of the Act is the key provision regulating Commonwealth government contracted service providers (it does not apply to ACT agencies). Generally, it provides that, in regards to a Commonwealth contract:

- it must contain provisions that ensure the contractor does not do an act that is inconsistent with the IPPs;

- it must not contain terms that authorise such an act;
- it must contain provisions that ensure that such an act is not authorised by a subcontract.

Where a contractor is overseas, the provisions of s 95B will generally continue to apply due to the Act’s extra-territorial provisions.

Drafting terms

Publications, guidelines and related materials

- Australian Government Solicitor, *Legal Briefing (No 63) – Outsourcing: Agency Obligations under the Privacy Act (2002)*
- OPC, *Private Sector Information Sheet 14 – 2001 Privacy Obligations for Commonwealth Contracts*

[45.35] The Commissioner has indicated that merely including a general clause requiring the contractor, for example, “not do an act, or engage in a practice, that would breach an Information Privacy Principle if done or engaged in by the agency” will not be sufficient to meet the requirements of s 95B. Generally, provisions will need to be more detailed and, in particular, specifically address how relevant requirements under the IPPs are to be met.

Two key resources have been published to assist agencies in taking appropriate contractual measures in agreements with service providers – see the documents listed in the “Publications, guidelines and related materials” box above. *Legal Briefing (No 63)* includes model contractual clauses.

In regards to including provisions to ensure subcontractors don’t breach the IPPs (required under s 95B(3)), this can be achieved by including terms that require the contractor to include written terms in the relevant subcontract that place the subcontractor under the same privacy obligations as the head-contractor. In many instances, however, government contracts prohibit the use of subcontractors, in which case such terms will not be required.

As far as the IPPs have no equivalent under the NPPs, a contractor that is otherwise normally bound by the NPPs will still be bound by the NPPs (see [45.55]). In view of this, the contract should specifically require the contractor to comply with NPP obligations so that:

- the agency has a contractual remedy available to it for any breach of the NPP obligations; and
- the contractor is made aware that these obligations remain in force.

Disclosures to contractors

[45.40] A disclosure of personal information by an agency must be in accordance with IPP 11 (“Limits on disclosure of personal information”). In most instances, disclosures to contractors will be authorised pursuant to one of the following two exemptions under IPP 11.1, provided the requirements of the exemptions are met:

- IPP 11.1(a) – where the individual concerned is reasonably likely to have been aware, or made aware under an IPP 2 privacy collection notice, that information of the relevant kind is usually passed to the contractor; and
- IPP 11.1(b) – where it is with consent (eg through signed consent forms).

Both exemptions require an agency to have taken certain steps prior to disclosing information to a contractor; namely, providing notice or obtaining consent. It is therefore essential that agencies foresee the disclosures they will need to make to contractors and either draft and provide collection notices or obtain consents accordingly.

Contractors that are small businesses

[45.45] If a contractor is a “small business operator” (eg it has annual turnover under \$3m), it generally will not be bound by the Privacy Act pursuant to the small business operator exemption under s 6C(1). However, if the contractor enters into a Commonwealth contract with an agency, it is prevented under the Act from being classed as a “small business operator” in relation to an act or practice engaged in for the

SAMPLE ONLY



Pages 2,644-4,400 are not part of this book preview.

[71]

Spam Act 2003 (Cth) – Guide and compliance manual

Introduction and overview	[71.05]
Coverage	[71.10]
Entities to which Act applies	[71.10]
“Electronic message”	[71.15]
Does not include a “voice call”	[71.20]
“Account”	[71.25]
“Electronic address”	[71.30]
“Internet carriage service”	[71.35]
“Listed carriage service”	[71.40]
“Message”	[71.45]
“Commercial electronic messages”	[71.55]
Must be for specified commercial purpose	[71.60]
Purpose determined based on content, presentation and links	[71.65]
Examples of commercial messages	[71.70]
Examples of non-commercial messages	[71.75]
“Business” and “investment” opportunities	[71.80]
Partnerships	[71.90]
Sending unsolicited messages	[71.110]
Prohibition	[71.110]
“Send”	[71.115]
“Australian link”	[71.120]
“Authorising” the sending of electronic messages	[71.125]
Exemptions	[71.130]
“Designated commercial electronic message”	[71.135]
Factual information	[71.140]
Government bodies, political parties, religious organisations and charities	[71.145]
“Government body”	[71.150]
“Charity” and “charitable institution”	[71.155]
“Religious organisation”	[71.160]
“Registered political party”	[71.165]
Educational institutions	[71.170]
Specified by regulations	[71.175]
Consent	[71.180]
Meaning of “consent”	[71.185]
Express consent	[71.190]
Inferred consent	[71.195]
Third party using account deemed to be authorised	[71.200]
Inferring consent from conspicuous publication	[71.205]
Withdrawal of consent	[71.210]
Unaware of Australian link	[71.215]
Mistake	[71.220]
Compliance guide	[71.225]
Sender information	[71.380]
Information to be included	[71.380]
Exemptions	[71.385]
Unaware of Australian link	[71.390]
Mistake	[71.395]
Compliance guide	[71.400]

Unsubscribe facility	[71.440]
Elements to be included in unsubscribe facilities.....	[71.440]
Exemptions	[71.445]
“Designated commercial electronic message”.....	[71.450]
Unaware of Australian link	[71.455]
Inconsistent with contract or agreement	[71.460]
Mistake.....	[71.465]
Compliance guide.....	[71.470]
General compliance issues	[71.565]
Reviewing messages, software and lists.....	[71.565]
Checklist: Reviewing types of commercial electronic messages sent	[71.570]
Reviewing types of software and lists used	[71.595]
Out-sourcing.....	[71.600]
Protecting against losses due to breach by contractor	[71.605]
Inclusion of information about out-sourcing party	[71.610]
Unsubscribe facilities	[71.615]
Does contractor’s exempt status apply to out-sourcer?	[71.620]
Does out-sourcer’s exempt status apply to contractor?	[71.625]
Government bodies, political parties, religious organisations, charities and educational institutions	[71.630]
Limitations of exemptions.....	[71.630]
Promotion of goods or services unrelated to entity’s core functions	[71.635]
Promotion of third party goods or services.....	[71.640]
Best practice and voluntary compliance	[71.645]
Exempt religious organisations and sensitive information	[71.655]
Removing logos and slogans from e-templates	[71.655]
Staff training.....	[71.660]
Preventing published addresses being used for spam	[71.665]
Relying on absence of Australian link.....	[71.670]
Complaint handling procedures	[71.675]
Contractual standards imposed by ISPs.....	[71.680]
Foreign laws	[71.685]
Staff working off-site	[71.690]
Miscellaneous	[71.700]
Enforcement	[71.700]
Enforcement – case summaries	[71.702]
Sending messages to non-existent addresses.....	[71.705]
Mailing lists – address-harvesting software and harvested address lists	[71.710]
Mailing lists – purchasing lists	[71.715]

SAMPLE ONLY



Pages 4,403-4,427 are not part of this book preview.

2. Consent

[71.180] The prohibition on sending commercial electronic messages does not apply if a relevant electronic account-holder has consented to receiving commercial electronic messages (s 16(2)). This is likely to be the exemption relied upon the most by businesses to continue sending marketing information to current and potential customers. The circumstances in which consent will be deemed to be given are addressed below.

Meaning of “consent”

[71.185] Consent is defined by the Act to mean (sch 2, pt 2):

- express consent; or
- consent that can reasonably be inferred from:
 - the conduct; and
 - business and other relationships;
 of the individual or organisation concerned.

Express consent

[71.190] Consent will be given where a person specifically states, either in writing or orally, that they consent to receiving commercial electronic messages. The Explanatory Memorandum to the *Spam Bill 2003* indicates that a recipient will also be deemed to have provided express consent to an organisation where, amongst other circumstances, they subscribe to the organisation’s electronic advertising mailing list, request (either verbally or in writing) advertising material or enter into an agreement to have their electronic address provided to a third party for marketing purposes (at p 113).

Inferred consent

[71.195] The definition of “consent” indicates that consent may be inferred not only from business relationships but also other types of relationships. For example, the Explanatory Memorandum provides that consent may be inferred from familial and other personal relationships; eg a business owner may send an email message to family and friends notifying them of a sale (at p 115). The Memorandum also indicates that consent to receive commercial electronic messages could be inferred, for example, where (at p 114):

- (a) a recipient has an existing business relationship with a sender and has knowingly and directly provided an electronic address to the sender;
- (b) a recipient provides his or her address when purchasing goods or services, unless in the circumstances a reasonable person would not expect to receive future messages (eg the recipient had merely provided the address for market research purposes, in which case it is indicated that it would not be reasonable to infer that consent has been given);
- (c) a recipient provides an electronic address with an expectation, or as a requirement, that it will be used in transactions and may also be used for additional communications (eg online banking);
- (d) a recipient registers a product or warranty online; or
- (e) a recipient provides a business card containing their electronic address to a commercial entity, unless in the circumstances a reasonable person would not expect to receive future messages (eg consent may not be implied in relation to messages that are not work related).

The Explanatory Memorandum indicates that the extent of the person’s consent will depend on what can be reasonably inferred from the conduct and relationship and will always be a question of fact to be determined based on the circumstances (at p 116). Examples of business relationships in which consent may reasonably be inferred include relationships between (p 115):

- an account-holder and retailer where the purchase of goods or services involves ongoing warranty and service provisions (eg a car with a warranty where the messages relate to the ongoing warranty and service of the car);
- a shareholder and both the company in which they hold shares and the stock broker;
- a magazine or newspaper subscriber and the relevant publisher;

SAMPLE ONLY



Pages 4,439-4,443 are not part of this book preview.

These steps will enable an organisation to take appropriate compliance measures in relation to each type of message based upon whether it is already exempt from the prohibition or whether consent needs to be obtained to bring it within the “consent” exemption (see [71.180]).

Checklist – Identifying exempt and non-exempt messages

The checklist below will assist in determining whether a particular type of commercial electronic message is subject to, or exempt from, the prohibition on sending commercial electronic messages.

1) Do the messages have an “Australian link”?

If not, the prohibition does not apply.

An organisation claiming that there is no Australian link will need to show that it has exercised reasonable diligence in ascertaining this – see [71.215].

For commentary on the meaning of “Australian link”, see [71.120].

2) Is the organisation a carriage service provider whose only connection with sending the messages is that someone else is using its services to send them?

If yes, the organisation is not deemed to send the messages and there are no compliance issues in relation to the prohibition – see [71.115].

3) Do the messages primarily contain factual information (eg a newsletter)?

If yes, the messages may fall within the “designated commercial electronic message” exemption – see [71.140]. However, such messages will still need to include sender information – see [71.380].

For commentary on what constitutes “factual information”, see [71.140].

4) Is the sender a government body, registered political party, religious organisation, charity or charitable institution?

If yes, most messages are likely to fall within the “designated commercial electronic message” exemption – see [71.145].

However, the exemption contains limits and, as such, only applies in certain circumstances (eg if the messages do not relate to goods or services, the exemption is not applicable). Consequently, certain messages sent by the entity may not be exempt. The body or organisation will need to develop a compliance strategy that enables messages that are not exempt to be identified to ensure that they are not sent in breach of the prohibition.

For commentary on the scope of the exemption, see [71.145].

The messages will still need to comply with the requirement to include sender information – see [71.380].

5) Is the sender an educational institution?

If yes, then, in many circumstances, messages sent by it will fall within the “designated commercial electronic message” exemption – see [71.170].

However, the exemption contains limits and, as such, only applies in certain circumstances (eg if the institution is not the supplier of the goods or services concerned, the exemption is not applicable). Consequently, certain messages may be subject to the prohibition. The institution will need to develop a compliance strategy that enables messages that are not exempt to be identified to ensure that they are not sent in breach of the prohibition.

In relation to the scope of the “educational institution” exemption, see [71.170].

6) Are the messages prescribed by regulations for the purposes of being a “designated commercial electronic message”?

If yes, the messages will fall within the “designated commercial electronic message” exemption – see [71.175].

7) Are the messages sent to persons who have consented (within the meaning of the Act) to receiving them?

The Act enables consent to be inferred in numerous circumstances – see [71.180]. These circumstances should be considered carefully as the “consent” exemption is relatively broad. If an intended recipient has consented, the messages will fall within the scope of the “designated commercial electronic message” exemption – see [71.180].

SAMPLE ONLY



Pages 4,445-5,200 are not part of this book preview.

Tort of invasion of privacy

Introduction	[80.10]
Australia	[80.20]
Developments towards establishment of tort	[80.20]
Queensland – <i>Grosse v Purvis</i>	[80.25]
Facts of case	[80.30]
Elements of action	[80.35]
Defences	[80.40]
Scope of action.....	[80.45]
Impact of decision.....	[80.50]
Victoria – <i>Doe v ABC</i>	[80.55]
England.....	[80.65]
New Zealand.....	[80.75]
Overview of position	[80.75]
Scope of rights protected	[80.85]
Stand-alone tort.....	[80.90]
Meaning of harm.....	[80.100]
Defence – legitimate public concern.....	[80.105]
Remedies	[80.110]

Introduction

[80.10] Traditionally, the common law has not recognised a right to privacy.¹ Consequently, individuals seeking civil remedies for interferences with their privacy have had to resort to related causes of action, such as breach of confidence, trespass, nuisance, defamation and intentional infliction of harm in order to seek redress.

However, in recent years, the development of a tort of invasion of privacy has gained significant momentum. The High Court has given the issue significant attention and has indicated a willingness to consider the development of such a tort in the future. Further, such a tort has been held to exist by lower courts; namely, the Queensland District Court and the Victorian County Court. However, it is far from clear whether a tort of invasion of privacy will be found to exist by superior courts in Australia.

Divergent paths have emerged in overseas jurisdictions. In England, information privacy interests are protected under extensions of the law of breach of confidence. In New Zealand, the same interests are protected under a stand-alone tort.

The federal Privacy Commissioner, the Australian Law Reform Commission and the NSW Law Reform Commission have each recommended in various reports (see [52.100]) that, in the absence of a tort of invasion of privacy at common law, a statutory tort should be established.

Notes

- ¹ *Malone v Metropolitan Police Cmr* [1979] 2 All ER 620 at 631 per Sir Robert-Megarry VC; *Kaye v Robertson* [1991] FSR 62 at 66, 70 and 71; (1990) IPR 147 at 150, 154 and 155; *R v Khan* [1996] 3 All ER 289.

Australia

Developments towards establishment of tort

[80.20] The High Court decision in *Victoria Park Racing and Recreation Grounds Co Ltd v Taylor* (1937) 58 CLR 479 has often been cited as authority that no right of privacy exists in Australia. In that case, it was held that a racecourse owner and operator could not prevent the observation and broadcasting of the progress and results of races on the racecourse by observers from a tower on land adjoining the course. Prior to *Victoria Park Racing* there had been some indications that a tort of invasion of privacy should be introduced (in *Church of Scientology v Woodward* (1982) 154 CLR 25 at 68 Murphy J identified “unjustified invasion of privacy” as a developing tort) but these were not followed in subsequent decisions (see *Cruise and Kidman v Southdown Press Pty Ltd* (1993) 26 IPR 125; *Australian Consolidated Press Ltd v Ettingshausen* per Kirby P at 15 (unreported, CA (NSW), BC9302147, 13 October 1993)).

However, in *Australian Broadcasting Corporation v Lenah Game Meats* (2001) 208 CLR 199, the High Court made it clear that *Victoria Park Racing* does not stand for any proposition respecting the existence of a tort of unjustified invasion of privacy, nor does it stand in the way of the development of such a cause of action. In that case, employees of Lenah, a processor and supplier of game meat, were secretly filmed lawfully slaughtering possums by members of the public. Lenah claimed that broadcasting the footage constituted an actionable invasion of Lenah’s privacy (despite the fact that Lenah was a body corporate), however, an injunction preventing ABC from broadcasting the film was lifted by the court. In their reasoning, the judges addressed the possible development of a tort of invasion of privacy.

In rejecting the proposition that *Victoria Park Racing* stood in the way of the development of a tort of invasion of privacy, Gummow and Hayne JJ commented (at 31-32) (with Gaudron J concurring) that the plaintiff in *Victoria Park Racing* was a corporation whose claim of breach of privacy was based solely on “pocket book” sensitivity which can be distinguished from a natural person seeking a right to privacy (see also at 89-91 per Callinan J) and that a corporation “lacks the sensibilities, offence and injury ... which provide ... staple value[s] for any developing law of privacy” (at 37) (notably, however, Callinan J indicated (at 93) that he would not rule out that, in certain circumstances, a corporation could enjoy a right to privacy).

Perhaps most significantly, Callinan J stated (at 95) that “... the time is ripe for consideration whether a tort of invasion of privacy should be recognised in this country ...”.

Significantly, Gleeson CJ considered that the English approach to breach of confidence (see [80.65]) was an appropriate means by which to protect the filming of private activities, citing with approval (at

SAMPLE ONLY



Pages 5,203-5,205 are not part of this book preview.

end, however, McLaughlan AsJ did not consider it necessary to conclude a view regarding the existence of a cause of action for invasion of privacy for the determination of the present application.

In *Batistatos v Roads and Traffic Authority of NSW; Batistatos v Newcastle City Council* [2006] HCA 27, Callinan J made comments that should offer encouragement to any party seeking to argue that a tort of privacy should be developed. In the context of a discussion about how innovative legal argument has often led to major changes in the law, Callinan J stated (at 216-217):

The truth is that in recent times, the courts, especially this Court have not always altered the law only incrementally ... I took the view in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd* that the time was ripe for the consideration at least of the recognition by the law of a cause of action for invasion of privacy. In view of the fact that my opinion was only a dissenting one, it is difficult to see how an advocate in New South Wales could seek to bring this matter before the courts now even though the law is moving in that direction in the United Kingdom. There has however been a civil case in Queensland where damages were awarded for invasion of privacy ... The truth is that the common law has often owed its development to, and has benefited from, the adventurousness and ingenuity of counsel.

These comments confirm the view that the fact that the development of a tort of privacy would represent a radical change in the law should not act as a barrier to such development.

The case of *Royal Women's Hospital v Medical Practitioners Board of Victoria* [2006] VSCA 85 offers a similar viewpoint. In that case, the Supreme Court of Victoria gave detailed consideration of the role and application of Article 17 of the International Covenant on Civil and Political Rights which provides "[n]o-one shall be subjected to arbitrary or unlawful interference with his privacy ...". Maxwell J stated that practitioners should be encouraged to develop human rights-based arguments where relevant to a question in the proceeding, should be alert to the availability of such arguments and should not be hesitant to advance them – see [88.20].

In *Chan v Sellwood* [2009] NSWSC 1335, Davie J observed that the position regarding the development of a tort of invasion of privacy in Australia is “a little unclear”. His Honour stated (at [37]):

Whether the law of Australia recognises a tort for breach of privacy is a little unclear. What the High Court said about it in *ABC v Lenah Game Meats Pty Ltd* [2001] HCA 63; (2001) 208 CLR 199 at [40]-[42] and [106]-[132] and [189]-[190] would not appear to preclude the emergence of such a tort. In *Grosse v Purvis* (2003) Aus Torts Reports 81-706 Skoien J of the Queensland District Court found that there was such a tort (see at [421]-[447]). Heerey J in *Kalaba v The Commonwealth* [2004] FCA 763 thought that the weight of authority was, at that time, against the proposition that there was such a tort but in *Gee v Burger* [2009] NSWSC 149 McLaughlin AsJ thought at [53] that the matter was arguable.

Queensland – *Grosse v Purvis*

[80.25] In *Grosse v Purvis* [2003] QDC 151, Senior Judge Skoien, of the District Court of Queensland, held (at [442]) that a civil action for damages based on the right of an individual person to privacy exists at common law.

However, whilst *Grosse* provides authority for the existence of a common law right to privacy, particularly in view of the High Court’s comments in *Australian Broadcasting Corporation v Lenah Game Meats* (2001) 208 CLR 199 (see [80.20]), courts in other jurisdictions may reject the case as bad law; for example, on the grounds that there is no clear authority from a superior court that such a right exists. *Grosse* has not been followed by the Federal Court, Supreme Court of Victoria or Supreme Court of South Australia in subsequent decisions involving alleged breaches of privacy – see [80.20].

Facts of case

[80.30] In *Grosse*, the plaintiff had a sexual relationship with the defendant. After the relationship ended, the defendant pursued and stalked the plaintiff by persistently loitering outside her places of residence and work, spying on her, entering her house without permission, coming into physical contact with her without consent, making offensive phone calls and acting in an offensive manner towards her friends and relatives. This behaviour continued over a period of several years, causing the plaintiff to suffer post traumatic stress disorder, affecting her ability to perform her duties at work.

In holding that an action for breach of privacy exists, the court awarded the plaintiff \$178,000 in damages, comprising:

- \$108,000 compensatory damages;
- \$50,000 aggravated compensatory damages; and
- \$20,000 exemplary damages.

Elements of action

[80.35] Senior Judge Skoien did not conclusively state the limits of the action for invasion of privacy, indicating that it was only necessary to state the essential elements as being (at paragraph [444]):

- (a) a willed act by the defendant,
- (b) which intrudes upon the privacy or seclusion of the plaintiff,
- (c) in a manner which would be considered highly offensive to a reasonable person of ordinary sensibilities,
- (d) and which causes the plaintiff detriment in the form of mental psychological or emotional harm or distress or which prevents or hinders the plaintiff from doing an act which [he or] she is lawfully entitled to do.

Senior Judge Skoien left the question open (at paragraph [446]) as to whether a defendant would be liable for negligent acts as opposed to willed acts.

Defences

[80.40] Senior Judge Skoien did not state any defences that will be available in an action for invasion of privacy, indicating that it was unnecessary to do so for the purposes of the case (at paragraph [444]). His Honour did, however, state that the defence of public interest should be available (at paragraph [447]).

In *Grosse*, the defendant effectively claimed that his acts should be regarded as lawful because, among other things, he believed he was doing them for the benefit of the plaintiff. Senior Judge Skoien indicated that it was unnecessary to decide whether a defence of actual intention to protect, or cause a benefit to, the plaintiff should be available, as such an intention did not motivate the defendant. However, his Honour commented (at paragraph [447]) that such a defence may be incompatible with the third element of the cause of action (that the relevant act be committed in a manner that would be considered highly offensive to a reasonable person of ordinary sensibilities).

Scope of action

[80.45] A key issue to be resolved in order to assess the scope of the rights afforded by the tort of invasion of privacy is the breadth of the meaning of “privacy” and, in particular, whether it encompasses rights in relation to information privacy, privacy of communications, surveillance, bodily privacy and privacy of space.

The defendant’s conduct in *Grosse* involved spying, loitering, trespassing and physical interferences with the plaintiff and, as such, related to rights of privacy from surveillance, bodily privacy and privacy of space. As the invasion of privacy was made out on these facts, “privacy” arguably encompasses at least these interests. It remains to be resolved whether the action is available in relation to interferences with rights relating to information privacy and privacy of communications.

If the common law right to privacy does encompass the full gamut of privacy rights, the rights afforded to individuals will be a significant addition to those already provided for under statute, particularly in view of the fact that it offers a civil remedy and of the level of damages that may potentially be awarded.

Impact of decision

[80.50] *Grosse* could have significant implications regarding the activities of individuals and businesses in Queensland. Businesses and areas of activity that could be impacted include:

- media organisations – due to their investigative and reporting techniques that could be deemed offensive by a reasonable person (although, the public interest defence proposed by Senior Judge Skoien may apply in this context);
- surveillance – any individual or organisation carrying out surveillance (for example, through the use of listening devices, video cameras, tracking devices and data surveillance devices) will need to ensure that it is not conducted in a manner that would satisfy the test set out in *Grosse*. In addition to organisations that have closed circuit television security systems, organisations that commonly undertake surveillance activities include insurance companies, private investigators and security companies.

Unless rejected, either in Queensland or in other jurisdictions, *Grosse* could result in an increase in privacy litigation, due primarily to the level of damages that could be available at common law.

Victoria – Doe v ABC

[80.55] In *Doe v Australian Broadcasting Corporation* [2007] VCC 281, Judge Hampel of the Victorian County Court “respond[ed] ... to the invitation held out by the High Court in [*ABC v Lenah Game Meats*]” and held that an invasion of privacy is an actionable wrong. It was the first case in any Australian jurisdiction since *Grosse v Purvis* [2003] QDC 151 (see [80.25]) to find that such a tort exists.

In *Doe*, the Australian Broadcasting Corporation, a reporter and a sub-editor were held liable in civil damages for naming the plaintiff as a victim of rape in breach of s 4(1A) of the *Judicial Proceedings Reports Act 1958* (Vic) (JPRA) which made it an offence to publish information identifying the victim of a sexual offence. The plaintiff based her case in the following causes of action: (i) breach of statutory duty; (ii) negligence; (iii) breach of confidence; and (iv) breach of privacy. The defendants were held liable on all grounds.

The defendants argued that the plaintiff should be limited to bringing a claim for defamation as the entire case was based on communication of information by the defendant to third parties. As such, in order to preserve the coherency of the law, the plaintiff should only be compensable in defamation proceedings. Judge Hampel rejected this argument, stating that the plaintiff was free to choose the actions in which she based her claims and the actions selected did not impose duties or obligations on the defendants inconsistent or incompatible with their rights, duties or obligations under defamation law (at [56]). Further, Judge Hampel concluded that the type of harm the plaintiff was claiming she had suffered was not the type of harm with which defamation is concerned, stating (at [64]):

This is not a case about defamation. The plaintiff is not complaining she has suffered a loss of reputation following publication of discreditable information about her ... The plaintiff's complaint is that the defendant published information which identified her, in the face of the [statutory] prohibition on publication of such information ... It is for the loss of the right not to have her identity published, and the harm flowing from the publication of information identifying her that she claims damages.

In relation to the claims for breach of duty and negligence, the court held the defendants had breached:

- s 4 of the JPRA and were liable in damages to the plaintiff; and
- their duty of care to the plaintiff to avoid causing her psychiatric injury through the negligent publication of information identifying her as the victim of a sexual assault in circumstances where such publication was prohibited.

In relation to the claim for breach of confidence, Judge Hampel relied on several English authorities. English laws of confidence have developed significantly in past years as a result of the fact that *Human Rights Act 1998* (UK) requires UK courts to take into account the rights enshrined in the *European Convention for the Protection of Human Rights and Fundamental Freedoms* (see [80.65]). The need for

SAMPLE ONLY



Page 5,209 is not part of this book preview.

elements of the tort, finding simply that the wrong committed in that case – namely, the publication of personal information in circumstances where there was no public interest in publishing it and where there was a prohibition on its publication – was sufficient. Further, her Honour did not make it clear why it was necessary to create a new tort of privacy when other laws arguably adequately protected the plaintiff's privacy interests in the particular case.

As the decision was by a lower court, its importance in terms of precedent is limited both within Victoria and, even more so, outside Victoria. However, the decision is significant as it provides another strong indication of the willingness of the courts to develop a tort of invasion of privacy.

Commentary on the state of the law regarding privacy in England and New Zealand is set at [80.65] and [80.75] respectively. US cases regarding privacy are not addressed here because, as noted by the High Court in *Magill v Magill* [2006] HCA 51, they are of limited relevance in the Australian context. In that case, three judges stated "... reliance on constitutional doctrines [of privacy] not known to Australian law casts a shadow over the applicability in Australia of the reasoning in the American cases generally" (at [75]).

Notes

- 1 Murray Gleeson, "Address to the National Press Club of Australia" (speech delivered at the National Press Club of Australia, Canberra, 20 August 2008). See also N Berkovic, "Why privacy just isn't what it used to be" *The Australian*, 22 August 2008.

England

[80.65] In England, there is no right to privacy at common law. However, the English courts have effectively developed a "privacy" jurisdiction by extending the laws of breach of confidence.

The failure to recognise a right to privacy has been highlighted by some judges as representing an inadequacy in English law. In *Kaye v Robertson* (1991) 19 IPR 147 journalists gained access to the hospital room of a television celebrity who was recovering from serious head injuries. The journalists proceeded to take photos and ask questions of the celebrity (despite the fact that he was in no condition to respond to such questions) which were intended to be published by a tabloid newspaper. Whilst the court granted an interim injunction on the basis of libel and malicious falsehood, Bingham LJ said (at 150):

This case nonetheless highlights, yet again, the failure of both the common law of England and statute to protect in an effective way the personal privacy of individual citizens. The defendant's conduct towards the plaintiff here was "a monstrous invasion of his privacy" ... If ever a person has a right to be let alone by strangers with no public interest to pursue, it must surely be when he lies in hospital recovering from brain surgery and in no more than partial command of his faculties. It is this invasion of his privacy which underlies the plaintiff's complaint. Yet it alone, however gross, does not entitle him to relief in English law.

Similar comments can be found in *R v Khan* (Sultan) [1997] AC 558, *Schering Chemicals Ltd v Falkman Ltd* [1982] QB 1 and *Morris v Beardmore* [1981] AC 446.

However, whilst courts have refused to acknowledge a right to privacy, English law has extended laws of breach of confidence to protect privacy interests. In England, there are now effectively two distinct actions for breach of confidence.

One is the traditional action in which information has been disclosed in circumstances giving rise to a duty of confidence.

The second gives a right of action in respect of the publication of personal information of which the subject has a reasonable expectation of privacy, irrespective of whether any duty of confidence exists, but only where that publication is, or is likely to be, highly offensive to a reasonable person and is not outweighed by public interest or freedom of expression values. Accordingly, in relation to the latter action, it is not necessary for a pre-existing relationship to exist between parties before a duty of confidence will be imposed – the nature of the subject matter or the circumstances of the defendant's activities may suffice to give rise to liability: see, for example, *Campbell v MGN Ltd* [2004] UKHL 22 at para 14 per Lord Nicholls of Birkenhead; *Venables v News Group Newspapers Ltd* [2001] 1 All ER 908 at 933. As observed by Laws LJ in *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804 at 807, in such cases, "...the law would protect what might reasonably be called a right of privacy, although the name accorded to the cause of action would be breach of confidence." However, some of these outcomes were based on obligations under the *Human Rights Act 1998* (U.K.) which came into effect in England in October 2000, incorporating the *European Convention for the Protection of Human Rights and*

Fundamental Freedoms 1950 into the domestic law (in *Douglas, Zeta-Jones v Hello! Ltd* [2003] 3 All ER 996; [2003] EWHC 786 (Ch), Lindsay J stated (at para 186) that the recent English authorities on this issue “...represent a fusion between the pre-existing law of confidence and rights and duties arising under the Human Rights Act”). Article 8 of the Convention provides that everyone has the right to respect for his private and family life, his home and his correspondence. Sections 3 and 6 of the Human Rights Act state that legislation must be given effect to, and courts must act, in a way that is compatible with the rights contained in the Convention.

In *Douglas, Zeta-Jones v Hello! Ltd* [2003] 3 All ER 996; [2003] EWHC 786 (Ch), Michael Douglas and Catherine Zeta-Jones had sold the exclusive publishing rights for photographs of their wedding to *OK!* magazine. Rival *Hello!* magazine obtained unauthorised pictures of the wedding which they published. Douglas and Zeta-Jones brought their action based on, amongst other things, breach of confidence, breach of the *Data Protection Act 1998* (U.K.) and interference with their privacy. On the first appeal, Sedley LJ held that the *European Convention for the Protection of Human Rights and Fundamental Freedoms 1950* and the *Human Rights Act 1998* (U.K.) as reinforcing a common law right to privacy. However, the decision was overturned on appeal. Lindsay J found in favour of Douglas and Zeta-Jones but on the grounds of breach of confidence. Lindsay J refused to hold that there is an existing law of privacy, stating (at para 229) that it would be wrong of him to do so in view of the fact that Douglas and Zeta-Jones were adequately protected by the law of confidence.

However, Lindsay J made it clear that he considers the development of a law protecting individuals’ privacy, in areas where existing laws do not, necessary but that this should be done by Parliament rather than the courts, stating (at para 229):

That inadequacy will have to be made good and if Parliament does not step in then the Courts will be obliged to....[I]f Parliament does not act soon the less satisfactory course, of the Courts creating the law bit by bit at the expense of litigants and with inevitable delays and uncertainty, will be thrust upon the judiciary.

On appeal, the English Court of Appeal reconfirmed in *Douglas v Hello!* [2005] EWCA Civ 595 that privacy interests in England will be protected under laws of confidence. However, that outcome was based on the application of European Community law and U.K legislation. In reviewing the question of privacy, the court followed the landmark decision of the European Court of Human Rights (ECHR) in *von Hannover v Germany* (24 June 2004). In that case, the ECHR considered whether photos of Princess Caroline of Monaco in public places infringed her privacy. The ECHR held that national courts of States bound by the Convention have a duty to protect privacy of individuals under Article 8. In applying this decision, the court found that it was under an obligation to interpret the Human Rights Act in a way that would protect individuals’ privacy and that the relevant cause of action under which to do this was breach of confidence. In view of this, it is likely that English courts will increase the level of protection afforded to privacy interests in the future by continuing to develop the laws of confidence in this manner. Importantly, the court also indicated that the original interlocutory injunction preventing *Hello!* from publishing the unauthorised photos should have been upheld as damages for mental distress resulting from the invasion of privacy was an inadequate remedy. As such, it is likely that injunctions will be awarded more readily by English courts in privacy cases, having significant implications for media organisations.

Other high profile cases involving extensions of (and refusals to extend) the law of confidence to protect privacy include: *Beckham and Another v MGN Ltd* (28 June 2001, QBD, unreported) (Beckhams obtained injunctions preventing the publication of photographs of the inside of their home); *A v B* [2002] 2 All ER 545; [2002] 3 W.L.R. 542 C.A (on appeal, publication of stories regarding the affairs of a captain of a Premier League Football team were allowed); *Campbell v MGN Ltd* [2004] UKHL 22 (Naomi Campbell awarded compensation for publication of photographs of, and information regarding, her attendance at Narcotics Anonymous meeting); *Sebastian Coe Case* (July 2004, unreported – public figure failed in attempt to prevent newspapers publishing details of affair following interview with mistress, held public interest in freedom of press and freedom of speech outweighed public interest in keeping information private – *Campbell v MGN* distinguished on grounds that it related to information regarding medical treatment, as opposed to an affair, and Coe could not expect right to keep information private); *McKennitt v Ash* [2005] EWHC 3003, upheld on appeal in *Ash v McKennitt* [2006] EWCA Civ 1714 (the defendant was enjoined from publishing information about the plaintiff, a folk music writer and singer, regarding her personal and sexual relationships, personal feelings in relation to her deceased fiancé, health, diet,

SAMPLE ONLY



Pages 5,222-5,650 are not part of this book preview.

International privacy directives, guidelines and standards

European Union [90.15]
APEC [90.20]
 APEC Privacy Framework [90.20]
 Cross-border privacy rules for corporations [90.25]
 Pathfinder Initiative [90.30]
OECD..... [90.35]
UNESCO [90.40]
Resolutions and declarations of world data commissioners [90.45]
Global Privacy Standard..... [90.50]

[90.10] Numerous international standards, directives, declarations and guidelines regarding privacy exist which could have relevance in the Australian context. For example, an Australian organisation operating on a regional or international basis may wish to ensure that its information management standards are consistent with those of foreign organisations or international best practice standards. This section provides an overview of key international instruments.

European Union

[90.15] Key European Union (EU) data privacy directives and opinions include:

- *EU Data Protection Directive 95/46/EC of 24 October 1995*;
- *EU Directive on Privacy and Electronic Communications of 12 July 2002* (adopted 15 December 1997);
- *Opinion 1/2004 on the level of protection ensured in Australia for the transmission of Passenger Name Record data from airlines* (adopted by Article 29 Data Protection Working Party on 16 January 2004).

Directive 95/46/EC generally restricts EU member states from disclosing personal information to nations that do not have what are deemed by the European Commission to be “adequate” privacy protections. The Commission itself has not yet determined whether Australia’s laws provide adequate protection, although, the EU Working Group has provided an opinion that the private sector provisions of the *Privacy Act 1988* (Cth) do not provide adequate protection. However, in Opinion 1/2004, the Commission concluded that, in relation to the processing of passenger name record (PNR) data transferred from EU airlines to Australian authorities, Australian law ensures an adequate level of protection within the meaning of Directive 95/46/EC.

Under Article 26(4) of Directive 95/46/EC, the Commission is able to decide that certain standard contractual clauses offer sufficient safeguards, authorising a transfer of personal data to a third country which does not have an “adequate” level of protection. The effect of this is that, generally, where EU organisations incorporate such standard clauses into a contract governing the transfer of personal data, the data can be transferred to an organisation in a non-EU country that does not have “adequate” protection. The Commission has approved two separate sets of standard contractual clauses. The first of these was approved by the Commission in 2001 in Decision 2001/497/EC whilst the second was approved in December 2004 in Decision C(2004)5271. The standard clauses are not compulsory nor are they the only lawful way of transferring data to countries outside the EU. Organisations using the clauses are able to choose which set of clauses they use. The second set of clauses was proposed by businesses believing they better suited business needs, eg those relating to litigation, allocation of responsibilities and auditing requirements. Each set of clauses, however, is considered to provide a similar level of data protection.

The UK Information Commissioner has issued detailed advice for UK organisations on how to transfer information to “non-adequate” countries. The advice relates to the *Data Protection Act 1998* which implements the *EU Data Protection Directive 95/46/EC*.

APEC

APEC Privacy Framework

[90.20] In November 2004, Asia-Pacific Economic Cooperation (APEC) Ministers endorsed the *APEC Privacy Framework* (Oct 2004) which generally aims to promote a consistent approach to information privacy protection in both private and public sectors across the 21 APEC nations, including Australia, whilst at the same time avoiding the creation of unnecessary barriers to information flows. The Framework establishes nine APEC Privacy Principles (APEC PPs). The Framework contemplates that the APEC PPs will be given effect in each APEC economy and provides specific guidance on both domestic and international implementation. APEC has summarised the Framework’s four primary goals as being to:

- develop appropriate privacy protections for personal information;
- prevent the creation of unnecessary barriers to information flows;
- enable multinational businesses to implement uniform approaches to the collection, use, and processing of data; and
- facilitate both domestic and international efforts to promote and enforce information privacy protections.

The APEC PPs are intended to be consistent with the core values of the OECD's 1980 *Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data* which the Framework considers represent "... the international consensus on what constitutes honest and trustworthy treatment of personal information" (at p 4). The APEC PPs are intended to provide clear guidance and direction to businesses in APEC economies on common privacy issues and how they impact upon the way legitimate businesses are conducted. An overview of the APEC PPs is set out below:

- (I) **Preventing harm** – protections should be designed to prevent the misuse of information in view of harm that may be caused to individuals;
- (II) **Notice** – this principle establishes notification requirements for when information is collected (similar to NPP 1.3);
- (III) **Collection limitation** – information collected must be relevant, fair, lawful and, wherever appropriate, with notice or consent (similar to NPPs 1.1 and 1.2);
- (IV) **Uses of personal information** – information should only be used for the purpose of collection and other compatible or related purposes unless there is consent, it is necessary to provide goods or services requested or is in accordance with law or other pronouncements of legal effect (similar to NPP 2.1);
- (V) **Choice** – where appropriate, individuals should be provided with clear and prominent mechanisms to exercise choice in relation to how their information is handled (similar to the type of information endorsed by the *Resolution on Improving the Communication of Data Protection and Privacy Information Practices* – see [117.40]);
- (VI) **Integrity of personal information** – regarding accuracy of information (similar to NPP 3);
- (VII) **Security safeguards** – regarding the security of information (similar to NPP 4);
- (VIII) **Access and correction** – regarding access and correction rights (similar to NPP 6);
- (IX) **Accountability** – When transferring information to another entity, whether domestically or internationally, consent should be obtained or due diligence should be exercised, and reasonable steps taken, to ensure that the recipient will handle the information consistently with the APEC PPs (similar in certain aspects to NPP 9).

Notably, the APEC PPs do not address several issues addressed by the NPPs, including openness (NPP5), identifiers (NPP 7) and anonymity (NPP 8).

In relation to coverage, the APEC PPs are similar in many respects to the NPPs. "Personal information" is defined to mean any information about an identified or identifiable individual. The APEC PPs apply to a "personal information controller" meaning a person or organisation who controls the collection, holding, processing or use of personal information, excluding a person or organisation who performs such functions at the instruction of another person or organisation (eg employees and agents). The APEC PPs are also excluded from applying to an individual who handles personal information in connection with their personal, family or household affairs. Further, the APEC PPs only have a limited application in relation to publicly available information, particularly in relation to the principles regarding "notification" and "choices".

The Framework does not, however, provide an exhaustive list of exemptions to the APEC PPs. Rather, it is envisaged that member economies will create their own exemptions based on domestic requirements. However, paragraph 13 of the Framework provides that any exemption to the APEC PPs created by member economies, including those relating to national sovereignty, national security, public safety and public policy, should be: (a) limited and proportional to meeting the objectives to which the exemptions relate; and (b) made known to the public or in accordance with law. As such, there is a broad scope for member economies to create their own exemptions to the APEC PPs.

Part IV of the Framework ("Implementation") provides guidance to member economies regarding how the Framework will be given effect in each member economy. In comparison with standard international instruments, the Framework provides little detail in relation to implementation issues, possibly weakening the potential impact of the APEC PPs. Section A of Part IV ("Guidance for Domestic Implementation") focuses on measures that member economies should consider in implementing the Framework domestically. It provides that implementation should be achieved by whatever means each member deems most appropriate, including through legislation, administrative decisions or industry self-regulation regimes. Different APEC PPs may even be implemented through different means (ie overall

SAMPLE ONLY



Pages 5,654-6,400 are not part of this book preview.

[126]

Consent

Introduction	[126.10]
What constitutes “consent”?	[126.20]
Express consent	[126.25]
Implied consent.....	[126.30]
Written vs verbal consent	[126.33]
Elements of consent.....	[126.35]
Obtaining consent	[126.45]
Common methods.....	[126.45]
When should consent be obtained?	[126.50]
Direct marketing	[126.55]
Technology specific consents	[126.55]
Opt in and opt out consents.....	[126.60]
Sample forms: opt in and opt out consents	[126.60]
Seeking consent after opt out	[126.70]
Withdrawal of consent	[126.75]
Bundled consents	[126.85]
Drafting consent forms	[126.95]
What types of consent should be obtained?	[126.105]
Overview	[126.105]
Health service providers	[126.110]

Introduction

[126.10] Privacy principles generally permit personal information to be used and disclosed for any purpose for which consent has been obtained from the individual concerned (Cth: NPP 2.1(b), IPPs 10.1(a), 11.1(b); NSW – IPP 10(a); NT - IPP 2.1(c); QLD - IPPs 10(1)(a), 11(1)(b); SA - IPPs 8(a), 10(a); Tas - PIPP 2(1)(b); Vic - IPP 2.1(b)). Under certain privacy statutes, consent is also required to collect sensitive information, which includes health information (Cth: NPP 10; NT - IPP 10.1(a); Tas - PIPP 10(1)(a); Vic - 10.1(a)).

The commentary below addresses issues relating to what constitutes consent and practical issues associated with obtaining consent.

What constitutes “consent”?

Publications, guidelines and related materials

- OPC, *Guidelines to the NPPs* (2001) at pp 22 (“Consent”)
- OICQ, *Privacy Guideline – Key concepts* at [2.0] (“Agreement and consent”)

[126.20] Privacy legislation often defines consent to include both express and implied consent. For example, the Privacy Act and health records statutes in the ACT and Victoria expressly define it this way (see s 6(1), s 4 and s 3 respectively). Commentary on the meaning of express and implied consent in the context of the Privacy Act is set out below.

Generally, a consent will be interpreted to extend only to the extent that the relevant collection, use or disclosure is necessary for the purpose for which consent is being provided. For example, if a patient consents to their GP disclosing their health information to a specialist, the GP cannot send the patient’s entire patient file to the GP. Rather, the GP can only send medical records that are relevant to the ailment being treated.

Express consent

[126.25] Express consent, which can be written or verbal, is provided when an individual directly states that they consent to their personal information being used or disclosed for a particular purpose, such as when they sign a privacy consent form.

Implied consent

[126.30] Consent may be implied where it is reasonable to conclude from a person's words or actions that they have provided consent; for example:

- if a person expresses interest in a business's services and provides a business card, it could generally be implied that the person consents to the business sending them information about its services;
- where an individual discloses health information to a health service provider during a consultation, consent will generally be implied for the provider to use and disclose that information for purposes evident from discussions during the consultation, such as to forward relevant records to a specialist (*GPPHS* p xii-xiii).

Whilst it is preferable to obtain written express consent, this will not always be possible or practical. In these types of instances, it will be necessary for an entity to assess whether it can conclude that implied consent exists in view of surrounding circumstances.

An entity will be in a strong position to show that consent for a particular use or disclosure was implied the more it can demonstrate that (*NPPG* pp 37-38):

- the individual was given details about uses and disclosures (eg in a privacy policy);
- the individual was given an opportunity to withhold consent (eg on an application form);
- the individual was aware of the consequences of giving consent;
- the disadvantages of giving consent were negligible; and
- the individual will not be disadvantaged by choosing to withhold consent at a later date.

Implied consent is not established merely because:

- there has been no objection from the person;
- the person would probably consent (eg to a disclosure to a family member);
- the relevant use or disclosure is advantageous for the person.

In relation to implied consent, the *Explanatory Memorandum to the Privacy (Private Sector) Amendment Bill 2000* provided in the context of NPP 2.1(b) (at [324]):

Implied consent could legitimately be inferred from the individual's failure to object to a proposed use or disclosure (that is, a failure to opt out), provided that the option to opt out was clearly and prominently presented and easy to take up. If the consequences for the individual of the use or disclosure were serious, however, the organisation would have to be able to demonstrate clearly that the individual could have been expected to understand what was going to happen to his or her information. In such circumstances it would generally be more appropriate to seek express consent.

An example of implied consent was provided in *Seven Network v Media Entertainment and Arts Alliance* [2004] FCA 637. In that case, a call centre identified itself to persons it contacted as the entity that had engaged its services and proceeded to collect sensitive information (for which consent was necessary) that was provided in response to questions it asked. Seven Network argued that, as the call centre pretended to be the respondent and did not make full disclosure as to what it was doing, there was no informed consent to the collection, however, this argument failed. It was held that consent had been provided (ie it was implied) as the questions asked were clear and each person had a choice as to whether or not to answer (at [54]).

Written vs verbal consent

[126.33] It is always preferable to obtain express consent wherever possible, particularly where significant privacy risks are involved in order to avoid ambiguity and because, without documentation, it can be difficult to prove consent was obtained. It can often be difficult attempting to conclude whether consent has been implied. For example:

- it will often depend on the relevant person's subjective views of a situation; and
- the entity may be unaware of surrounding personal circumstances which, if known, would indicate consent is not implied (eg separation from a spouse would indicate there is no implied consent to disclose information to the spouse that might otherwise be present).

If an entity accepts verbal consents, policies should be developed regarding:

- uses and disclosures for which consent will not be accepted verbally;
- ID verification requirements (eg when provided over the phone);
- documenting such consents (eg the relevant officer must make a written note of the date, time, location, preceding conversation and other relevant circumstances surrounding the giving of consent).

Elements of consent

Publications, guidelines and related materials

- OPC, *Information Sheet 24 – Disclosure of health information and impaired capacity* (2008)
- PrivacyNSW, *Best Practice Guide – Privacy and People with Decision-making Disabilities* (2004)

[126.35] The general law applicable to consent is generally unaffected by privacy legislation, including the Privacy Act. Consequently, the requisite elements of consent must be met, including voluntariness, capacity to understand, capacity to provide and capacity to communicate.

The Privacy Commissioner has expressed the view that, to be valid, consent must be (*IPPG* at pp 24-26):

- voluntary – examples of involuntary consent may include:
 - where consent was provided under pressure from family members;
 - where withdrawal of a benefit is threatened unless consent is given;

SAMPLE ONLY



Pages 6,404-6,450 are not part of this book preview.

[132]

Access and correction

Publications, guidelines and related materials

- OICQ, *Information sheet - Evidence of authority and identity*
- Commentary on access and correction under NPP 6 (“Access and correction”) at [3.1205] and IPP 6 (“Access to records containing personal information”) at [5.330]

[132.10] Privacy principles and other provisions under privacy legislation generally provide individuals with rights to access and correct personal information an entity holds about them (see, eg: Cth: NPP 6, IPP 6, 7; NSW - IPP 7, 8; NT - IPP 6; QLD - IPP 6, 7; SA - IPP 5, 6; Tas – PIPP 6; Vic - IPP 6). There is a large variation in the number of requests for access and correction that entities receive, often depending on industry. For example, health service providers tend to receive a large number of such requests, whereas many businesses (even large corporations) receive few, if any, such requests.

Entities, particularly those that receive regular requests for access and correction, should have in place procedures and forms for the lodgement and processing of request for access and correction.

Privacy principles relating to access and correction generally set out various grounds on which an entity is entitled to deny a request for access or correction. Once a request has been lodged, an entity should have in place a process whereby it is vetted to see if, firstly, there is any reason as to why the entity may wish to refuse the request and, if so, to assess whether any exemptions can be relied upon to deny the request.

Where fees are charged for processing requests for access, applicants should be notified of the fees prior to processing of the application.

For commentary relating to the provision of access and correcting records under NPP 6 and IPPs 6 and 7 of the Privacy Act, see [3.1200], [5.330] and [5.330] respectively.

Sample forms for requests for access and correction are set out below.

Sample form: Request for access

Request for access to personal information

Privacy notice. We will use the information you provide to process your request for access.

We may disclose the information to any third parties involved in providing you access, such as courier service providers. If you do not provide the information requested on this form, we may be unable to process your application. You may request access to the information we collect about you at any time.

Applicant’s details

Title: Mr/Mrs/Miss/Ms

First name:

Surname:

You must provide evidence of your identity.

Agents/authorised representatives

If an agent or other authorised representative is requesting access on behalf of the applicant (eg solicitor or family member), the representative must provide the details below.

Title: Mr/Mrs/Miss/Ms

First name:

SAMPLE ONLY



Pages 6,452-6,600 are not part of this book preview.

Outsourcing

Introduction	[138.10]
Application of Act to contractors	[138.20]
Notification of disclosures	[138.30]
Contractors not bound by Act	[138.40]
Sensitive information.....	[138.50]
Checklist: privacy issues to address in contracts	[138.60]

Publications, guidelines and related materials

- OPC, *Information Sheet (Private Sector) 8 – 2001: Contractors*
- OPC, *Guidelines to the NPPs* (2001) at pp 22-23 (“Contractors”)
- OVPC, *Outsourcing and Privacy: A guide to compliance under the Information Privacy Act* (2011)
- AMSRS and AMSRO, *Guidelines for the contracting out of research services*
- OICQ, *Privacy Guideline – Contracted service providers*
- Commentary on contracted service providers (public sector) at [45]

Introduction

[138.10] Special issues arise when engaging contractors to provide services and, as part of the provision of those services, the contractors may access and acquire personal information held by the outsourcing entity. The commentary below addresses issues that arise specifically in the context of private sector organisations under the *Privacy Act 1988* (Cth). Many of the matters canvassed, particularly the checklist of issues to address in contracts with service providers (at [138.60]), will, however, be relevant to entities bound by other legislation.

Two key resources have been published providing guidance on addressing privacy issues with contractors:

- OPC, *Information Sheet (Private Sector) 8 – 2001: Contractors* – this publication provides guidance specifically in the context of the NPPs;
- OVPC, *Outsourcing and Privacy: A guide to compliance under the Information Privacy Act* (2011) – This publication provides detailed guidance on matters such as managing risks in, and checklists for entering into, outsourcing arrangements for both outsourcing entities and contractors in the context of the *Information Privacy Act 2000* (Vic).

For commentary relating to contracted service providers to Commonwealth agencies, see at [45].

Application of Act to contractors

[138.20] Where a private sector organisation (“outsourcer”) out-sources a function to a contractor and, in doing so, discloses to or collects personal information from the contractor, both the outsourcer and the contractor must, if they are both bound by the Privacy Act, comply with the NPPs in their own rights. In other words, an outsourcer and its contractor are regulated separately. Consequently, where, for example, an outsourcer forwards personal information to a contractor, the outsourcer is deemed to be disclosing the information and the contractor is deemed to be collecting the information and each entity must respectively disclose and collect the information in accordance with the NPPs.

Examples of service providers commonly engaged by organisations include: IT service providers, archival storage services, security companies, document destruction businesses, mailing houses, call centres and professional advisors (eg accountants). In the context of health service providers, these may include visiting and fee-for-service health professionals, ambulance service providers and pharmaceutical companies.

This distinction between an outsourcer and contractor was demonstrated in *B v Charity Organisation* [2010] PrivCmrA 3. In that case, the complainant received a letter addressed to them at their address from a charity asking them to provide further personal information and to support the charity. The complainant complained that the charity should not have collected and used their personal information given they had no previous dealings with the charity. The charity had outsourced its marketing activities to a third party contractor and, as such, had not itself collected or used the complainant’s information. Therefore, while the charity had provided the template for the letter to the contractor, the contractor had used its own database of customers to generate the name and address on the letter. The contractor did not provide this database to the charity. The Commissioner found that there had been no breach of the NPPs by the charity as it had not collected the complainant’s personal information or unlawfully used it to direct market them. If the complainant was to lodge a complaint, it needed to be against the contractor.

Where a contractor acts as agent for the outsourcer, it may be necessary to take additional compliance steps; for example, to notify customers that it is acting as agent and will disclose information to its principal. However, an agent’s obligations under the NPPs will vary according to the specific

SAMPLE ONLY



Page 6,603 is not part of this book preview.

- outline specific standards and information handling procedures and practices that must be observed in relation to various aspects of the information life cycle – these specific terms should be included (as opposed to solely requiring compliance with the NPPs) as, in many instances, contractors will be unaware of their obligations under the NPPs.

Sensitive information

[138.50] In many instances, NPP 10 will require an organisation to have consent to collect sensitive information. Accordingly, a contractor (if it is bound by the Act) must ensure consent is present for it to collect the sensitive information from the outsourcer. Likewise, where a contractor collects sensitive information on behalf of the outsourcer (eg a contractor, such as a telemarketer, deals with the outsourcer’s customers directly – see, for example, *Seven Network v Media Entertainment and Arts Alliance* [2004] FCA 637), the outsourcer must ensure that it has consent to collect the sensitive information from the contractor. This can be achieved by ensuring appropriate privacy collection notices and consent forms or terms are in place.

Checklist: privacy issues to address in contracts

[138.60] A checklist of key issues that should be considered and, where relevant, addressed in agreements with contractors is set out below.

Issues commonly addressed by privacy terms in contracts include:

- **Compliance with privacy laws and standards** – The service provider should be required to comply with relevant statutes (eg Privacy Act, health records statutes and *Spam Act 2003* (Cth)) regarding the manner in which it handles personal information in order to provide a contractual remedy for any breaches of the legislation. If the service provider is not bound by a relevant statute (eg the Privacy Act because it is a small business operator), the contract should provide that the service provider must comply with the relevant Act as though it were bound by it.

The service provider should also be required to comply with any additional information handling requirements, standards or policies (eg information management and IT security policies) the principal wishes to impose on the service provider. These may relate to information management practices generally or specific elements of them (eg staff training requirements).
- **Collection** – If the service provider collects personal information on behalf of the principal, the service provider should be required to provide any privacy notices to and obtain any privacy consents from individuals as reasonably required by the principal.
- **Use** – The purposes for which the service provider can use the personal information should be restricted to, for example, use solely for providing the services, unless the principal approves otherwise.
- **Disclosures** – The purposes for which the service provider can disclose the personal information should be restricted. Permitted disclosures may, for example, include:
 - those permitted by the agreement;
 - to the principal;
 - to subcontractors;
 - to the extent necessary for the purpose of providing the services;
 - as required law;
 - with the principal’s prior approval.
- **Data security** – The service provider should be required to ensure that the personal information stored by it or which is under its control is protected from misuse and loss and from unauthorised access, modification or disclosure; for example, by:
 - ensuring it is protected by the same information security controls protecting information held within its own data processing and information handling systems;
 - developing, implementing and maintaining appropriate administrative, technical and physical security measures that meet industry standards;

SAMPLE ONLY



Pages 6,605-7,100 are not part of this book preview.

[159]

Video surveillance

Introduction	[159.10]
Surveillance devices legislation	[159.13]
Information privacy statutes.....	[159.16]
Surveillance images as personal information.....	[159.20]
Exemptions	[159.30]
Key compliance issues.....	[159.40]
Common law	[159.50]

Introduction

[159.10] Numerous statutory and common law sources impact on the use of video surveillance devices. The commentary below summarises sources of regulation and compliance risks.

Surveillance devices legislation

[159.13] Video surveillance is directly regulated by:

- listening and surveillance devices legislation (listening devices legislation will be applicable where video cameras also make sound recordings) – see [72.10]; and
- workplace surveillance legislation – see [73].

Accordingly, the manner in which video surveillance is conducted in those jurisdictions must be in accordance with applicable surveillance devices and workplace surveillance statutes.

Information privacy statutes

[159.16] Information privacy statutes, such as the Privacy Act, impact on video surveillance where images captured by cameras constitute personal information within the meaning of the relevant statute. In these circumstances, the legislation regulates the collection, use, storage and disclosure of the surveillance images. However, in practice, video surveillance is rarely the subject of privacy complaints. In 2009, the Privacy Commissioner indicated that only around two per cent of enquiries it receives have related specifically to surveillance issues (*Privacy Matters* (OPC), Summer 2009). The most common issues that individuals raise relate to the use of surveillance devices in a workplace setting, covert surveillance by insurers in relation to claim assessments and use of surveillance devices (such as web cams, home-based video monitoring systems) by individuals acting in a private capacity.

Surveillance images as personal information

[159.20] Under information privacy statutes, personal information is generally defined sufficiently to include images where a person’s identity can be reasonably ascertained from it. For example, under the Privacy Act, personal information is defined to mean (s 6(1)):

[I]nformation or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.

Under this broad definition, personal information extends to pictures of an individual in a video surveillance image where the individual’s identity is apparent, or could be reasonably ascertained, from the image. The mere fact that the information does not itself reveal the individual’s identity does not mean that it is not personal information as the image could be matched with other information (eg the individual’s photo identity card or a client database) that enables the individual to be identified. Consequently, whether the individual’s identity

can be “reasonably ascertained” from the image will depend largely on the resources available to the organisation that could enable it to identify the individual. For example, in the context of CCTV surveillance in a bank, a bank will often be able to readily identify individuals in video footage by linking images with transaction and account details.

Exemptions

[159.30] Where video surveillance constitutes personal information, the entity that has conducted the surveillance will be entitled to rely on any exemptions available under the relevant privacy statute. For example, under the Privacy Act, where a private sector organisation has conducted workplace surveillance of employees, the surveillance footage will generally be subject to the employee records exemption (see [14.140]).

Similarly, privacy statutes often contain exemptions permitting entities to use or disclose personal information for the purpose of investigating suspected unlawful activity (see, eg, NPP 2.1(f)). This type of exemption is particularly relevant in view of the fact that surveillance is often carried out in an attempt to prevent, or obtain evidence of, criminal activities. Similar exemptions often exist permitting use or disclosure for the purpose of assisting law enforcement agencies (see, eg, NPP 2.1(h)).

Key compliance issues

[159.40] Key privacy compliance issues associated with video surveillance that captures personal information are addressed below.

- **Collection** – The recording of images from video surveillance cameras must generally be necessary for one of the entity’s functions or activities (Cth: NPP 1.1, IPP 1; NSW - IPP 1(b); NT - IPP 1.1; QLD - IPP 1(1)(b); Tas - PIPP 1(1); Vic – IPP 1.1). Accordingly, it is generally necessary to ensure that the images that are being captured are relevant to the purpose of surveillance. In many instances, surveillance will be carried out for security purposes. It may, however, also be conducted for other purposes, such as monitoring of staff.

Surveillance cameras generally must not be used to capture images that are collected in an unfair or unreasonably intrusive way (see, eg, Cth: NPP 1.2, IPPs 1, 3; NT - IPP 1.2; QLD - IPP 1(2); SA - IPP 1; Vic - IPP 1.2). Depending on the circumstances, the use of hidden cameras may or may not be considered unfair. For example, secret surveillance in a hotel lobby is likely to be deemed to be unfair as there is little need for the surveillance to be secret. On the other hand, the Privacy Commissioner has indicated that it is generally not unfair for information to be collected secretly where it is for the purpose of an investigation of suspected unlawful conduct (see [3.65]). This would be likely to include, for example, a private investigator conducting secret surveillance during an investigation of a suspected fraudulent insurance claim. An organisation must ensure that surveillance cameras are positioned appropriately. Generally, surveillance of areas that a reasonable person would not expect to be kept under surveillance are likely to be considered unreasonable. For example, the positioning of cameras to capture images in toilet cubicles or at urinals will generally be unreasonably intrusive. However, in appropriate circumstances, it could be acceptable to position cameras to capture images at basins, in front of cubicle doors and drinking troughs, for example, where it is to detect illegal activity. In *Mildenhall v Department of Education* [1998] VCAT 465 (Victorian Civil and Administrative Tribunal, 23 October 1998), cameras were placed in school toilets to capture images at basins, in front of cubicle doors and drinking troughs of suspected drug dealing, although the positioning of the cameras was not in issue in that hearing.

At or before taking surveillance footage that captures personal information about individuals, or as soon after as is practical, an entity is generally required to take reasonable steps to ensure that those individuals are aware of certain information, such as the organisation’s identity and contact details, purpose of collection, rights of access and the organisations, or the types of organisations, to which such footage is usually disclosed (Cth: NPP 1.3, IPP 2; NSW - IPP 3; NT - IPP 1.3; QLD - IPP 2; SA - IPP 2; Tas - PIPP 1(3); Vic - IPP 1.3). It will generally not be practical for an entity to inform an individual of this information before the time of surveillance. Consequently, the entity must take reasonable steps to inform the individuals either at, or as soon as is practical after, the time of surveillance. Reasonable steps are likely to include placing clearly visible signs on

SAMPLE ONLY



Pages 7,103-8,100 are not part of this book preview.

[205]

Data security

Introduction	[205.10]
Reasonable steps to secure information	[205.20]
Security standards	[205.30]
Checklist: Data security risks and control measures	[205.40]
Hardcopy and electronic records	[205.40]
Hardcopy records.....	[205.40]
Electronic records	[205.40]
Portable storage devices	[205.70]
Introduction	[205.70]
Checklist: Security risks and control measures.....	[205.75]
Data security breaches and notification.....	[205.85]
Data destruction.....	[205.95]
Overview	[205.95]
“Reasonable” steps to destroy.....	[205.100]
Secure destruction methods – hardcopy and electronic media.....	[205.105]
Cases	[205.115]

SAMPLE ONLY



Pages 8,102-8,103 are not part of this book preview.

Checklist: Data security risks and control measures

Hardcopy and electronic records

Issue	Guidance
Information security policies	<p>Entities should establish and implement information security policies that appropriately address data security risks. This can be done through an overarching Information Security Policy covering both hardcopy and electronic records which references other documentation which may support the policy, eg more detailed security policies and procedures relating to specific practices or systems.</p> <p>In addition to an Information Security Policy, examples of policies through which data security risks are commonly addressed include:</p> <ul style="list-style-type: none"> • Information Management Policy • IT Security Policy • Portable Storage Devices Policy • Electronic Records Disposal Policy • Password Policy • Remote Access Policy • Cryptographic Policy • Acceptable Usage Policy (Internet & Email) • Document Retention Policy
Information security responsibilities	<p>Overall responsibility for information security should be assigned to one or more appropriately qualified and experienced senior officers (eg Chief Information Officer, Information Security Manager, Records Manager, Privacy Officer).</p>
Information classification	<p>Appropriate policies (eg Information Security Policy) should classify information, including in particular personal information, into appropriate categories, such as “highly confidential”, “confidential” and “public”, and establish rules and procedures regulating how each category may be handled.</p>
Employees	<p>The following security measures should be taken in relation to employees:</p> <ul style="list-style-type: none"> • employees should be required to comply with data security policies and procedures through employment contracts; • ensure job descriptions clearly specify data security responsibilities; • where appropriate (eg in relation to high risk data), have “job handover” notes address privacy issues; • where appropriate, background checks and police clearances obtained prior to allowing access to systems and information; • ensure employment contracts require employees to return all records containing personal data upon or prior to termination of employment (and ensure such term survives termination of the contract); • confidentiality/non-disclosure agreement covering personal data (including after termination of employment); • ensure policies are enforced regularly and consistently; • a formal disciplinary process should be in place for employees who have committed a security breach to ensure policies are enforced; • an appropriate policy should prohibit staff accessing, copying, modifying, using and/or removing personal data for any purpose other than a work purpose.
Contractors	<p>Where contractors access or handle personal information on behalf of an outsourcing organisation, contractual measures should be taken to ensure the</p>

SAMPLE ONLY



Page 8,105 is not part of this book preview.

Hardcopy records

Issue	Guidance
Storage	<p>Physical security measures prevent unauthorised access to information held in documents and are relevant to all forms of storage. Physical security measures include lockable drawers, lockable filing cabinets and compactuses, placement of filing cabinets in locked rooms, safes and lockable storage containers. The quality or security grading of storage facilities (eg of locking mechanisms and filing cabinets) should be higher for high risk documents.</p> <p>Whether it is appropriate to leave lockable facilities unlocked during business hours will depend largely on the sensitivity of the documents they contain – the more sensitive the documents, the more reasonable it will be to leave the facilities locked at all times.</p> <p>Where offices are open plan and there is no physical separation between departments, this will result in an increased need for lockable storage facilities to reduce the risk of non-departmental staff accessing documents without authority.</p>
Access controls	<p>Information management systems should incorporate procedural and physical access controls to ensure documents are protected from unauthorised access, modification and disclosure.</p> <p>Such controls should be used to ensure staff only access documents on a need-to-know basis having regard to their work functions. In addition to physical controls, procedural measures (which establish a disincentive of disciplinary action if breached) are of particular importance in the context of hardcopy documents as access logs are often impractical in relation to such records (unlike electronic records).</p>
Clear desk policy	<p>To reduce the risk of unauthorised access to documents during and outside business hours, a clean desk policy (requiring, for example, that documents not be left on unattended desks or that staff file documents away when leaving the office) should, where appropriate, be adopted in relation to documents containing personal information. The circumstances in which such a policy should be adopted, and its scope, will depend on factors such as the sensitivity of the documents, the risk of attempts at unauthorised access being made, the number of people who have access to desks (often a large number in open plan offices with no physical separation between departments) and practicality for staff.</p>
Transfer and communications	<p>Documents should be protected against unauthorised access and misuse when being transported:</p> <ul style="list-style-type: none"> • Where high risk documents, or large numbers of documents containing personal information (eg storage containers containing large numbers of customer files), are sent off-site using third party service providers, they should only be sent using reliable service providers and transferred by signed receipt delivery services (eg Australia Post’s registered post service) or equally secure means (eg in person) to reduce the risk of them being lost in transit, intercepted and being delivered to incorrect recipients. In some instances, additional security measures may be appropriate; for example, use of locked containers and tamper-evident packaging. • Whilst use of signed receipt delivery services can significantly increase postage costs and be relatively time consuming (as it

SAMPLE ONLY



Page 8,107 is not part of this book preview.

Electronic records

Issue	Guidance
Asset management – asset inventory	<p>From a privacy perspective, an inventory log of all IT assets storing personal data (eg computers, laptops, USB flash drives, DVDs, digital photocopying machines) should be maintained and regularly checked and updated (at least annually) to:</p> <ul style="list-style-type: none"> • enable instances of loss or theft to be identified and investigated; and • ensure decommissioned devices are handled in accordance with records destruction policies.
Computer and network security (access controls)	
	<p>Audit logging and monitoring system usage</p> <p>Automated audit trails should be implemented to record user activities to ensure instances of inappropriate access, use and modification can be traced.</p> <p>Audit logs should, at a minimum, log: user IDs; dates, times, and details of key events, eg successful login and logout; unsuccessful login; terminal identity or location; use of and failed attempts to use system privileges, utilities and applications; access, add, change, delete or transfer a file. The Privacy Commissioner has indicated in numerous cases that this is a key security measure large organisations must have in place.</p> <p>Logs should be secured so they cannot be altered (other than, if unavoidable and/or appropriate, by IT security managers).</p> <p>Logs should be regularly monitored and reviewed to monitor for instances of unauthorised access or modification and compliance with policies.</p>
	<p>Unattended equipment</p> <p>Password protected screen-lockouts on computers and terminals should be used which automatically initiate after a short period of inactivity (eg 5-15 mins) having regard to risk levels involved.</p> <p>Session time-out should be implemented for both the network and individual applications storing personal information. A time-out facility should clear the session screen and also, possibly later, close both application and network sessions after a defined period of inactivity. Users should be required to log back in to recommence or continue their session after a short period of inactivity (eg 5-15 mins) having regard to risk levels involved and other relevant considerations, such as practicality for staff.</p>
	<p>Passwords</p> <p>A Password Policy should be adopted addressing user ID and password requirements to authenticate user identities (note: other measures can be used to authenticate users, such as smart cards and biometrics – not addressed here). The Password Policy should, among other things, address the following issues:</p> <ul style="list-style-type: none"> • passwords should be unique to each user ID (ie there should be no group/shared passwords); • password storage – passwords should not be stored in non-secure locations (eg near computers); • password confidentiality – staff should be required to treat passwords confidentially and prohibited from disclosing them to anyone under any circumstances. If, in special circumstances, a disclosure is necessary, the password should

SAMPLE ONLY



Pages 8,109-8,124 are not part of this book preview.

Portable storage devices

Publications, guidelines and related materials

- OPC, *Information Sheet (Public Sector) 3 – Portable storage devices and personal information handling*
- OVPC, *Use of Portable Storage Devices: A Guide to Policy Development (2009)*
- OICQ, *Information sheet – Portable storage devices and information privacy*

Introduction

[205.70] A portable storage device (PSD) is any small, lightweight, portable device capable of storing and transferring large volumes of data (eg external hard drives, CDs/DVDs, USB flash drives, laptops, BlackBerries, MP3 players and mobile phones). PSDs storing data pose a major data security risk by virtue of their portability and subsequent risk of being lost or stolen (particularly when taken off-premises), resulting in unauthorised disclosures.

In view of the extreme high data security risk posed by PSDs, entities should, in addition to other IT security policies, adopt a portable storage device policy to specifically address risks posed by PSDs. This will assist in achieving compliance with obligations under data security privacy principles (Cth: NPP 4, IPP 4; NSW - IPP 5; NT - IPP 4; QLD - IPP 4; SA - IPP 4; Tas - PIPP 4; Vic - IPP 4). For a checklist of issues that should be addressed in such a policy, see below at [205.75].

The federal Privacy Commissioner, Victorian Privacy Commissioner (OVPC) and Queensland Information Commissioner have each published guidelines regarding the management of PSDs and, in particular, the development of policies and procedures relating to the handling of PSDs and how to safeguard personal information stored on them. The documents relate to public sector agencies, however, are equally relevant to private sector organisations and should be consulted when developing policies in relation to PSDs. The respective guidelines are outlined in the “Publications, guidelines and related materials” box above.

Checklist: Security risks and control measures

[205.75] A Portable Storage Device policy should apply to all PSDs and all users (including staff, contractors, consultants, interns, volunteers and visitors) and be flexible enough to apply to new types of PSDs.

Issues that should be addressed in a Portable Storage Device Policy are outlined below.

Work issued devices

- **risk assessment** – regular risk assessments of each type of PSD should be conducted to determine the risk level and appropriate security measures.
- **limitation of data storage** – restrictions should be placed on what data can be stored on PSDs. Generally, such data storage should not be permitted unless absolutely necessary. Data that can be so stored should be restricted to the minimum necessary for the relevant purpose.
- **personal use** – whether, and in what circumstances, work PSDs may be used for personal use.
- **prompt transfers from PSD to network** – where appropriate, personal data should be required to be transferred from PSDs to the workplace network as soon as possible and the data deleted from the PSDs.
- **data transfers to other devices** – policy and/or technical measures should restrict transfers of data to other PSDs (eg removing USB ports on laptops and disabling wireless access for devices not designated for wireless purpose).
- **blocking USB ports** – whether, and in what circumstances, workstation USB ports should be disabled, removed or blocked or use non-standard locking ports (generally, such measures should only be used where there are significant risks associated with PSDs as they may prevent staff from legitimately using work issued PSDs).
- **handling off-site** – staff should be made responsible for the physical security of PSDs in their care

SAMPLE ONLY



Pages 8,126-8,628 are not part of this book preview.