# List of Recommendations

## Part A—Introduction

## 3. Achieving National Consistency

**Recommendation 3–1** The *Privacy Act* should be amended to provide that the Act is intended to apply to the exclusion of state and territory laws dealing specifically with the handling of personal information by organisations. In particular, the following laws of a state or territory would be excluded to the extent that they apply to organisations:

(a) *Health Records and Information Privacy Act 2002* (NSW);

(b) *Health Records Act 2001* (Vic);

(c) *Health Records (Privacy and Access) Act 1997* (ACT); and

(d) any other laws prescribed in the regulations.

**Recommendation 3–2** States and territories with information privacy legislation that purports to apply to organisations should amend that legislation so that it no longer applies to organisations.

**Recommendation 3–3** The *Privacy Act* should not apply to the exclusion of a law of a state or territory so far as the law deals with any 'preserved matters' set out in the Act. The Australian Government, in consultation with state and territory governments, should develop a list of 'preserved matters'. The list should only include matters that are not covered adequately by an exception to the model Unified Privacy Principles or an exemption under the *Privacy Act*.

**Recommendation 3–4** The Australian Government and state and territory governments, should develop and adopt an intergovernmental agreement in relation to the handling of personal information. This agreement should establish an intergovernmental cooperative scheme that provides that the states and territories should enact legislation regulating the handling of personal information in the state and territory public sectors that:

(a) applies the model Unified Privacy Principles (UPPs), any relevant regulations that modify the application of the UPPs and relevant definitions used in the *Privacy Act* as in force from time to time; and

(b) contains provisions that are consistent with the *Privacy Act*, including at a minimum provisions:

(i) allowing Public Interest Determinations and Temporary Public Interest Determinations;

(ii) regulating state and territory incorporated bodies (including statutory corporations);

(iii) regulating state and territory government contracts;

(iv) regulating data breach notification; and

(v) regulating decision making by individuals under the age of 18.

**Recommendation 3–5** To promote and maintain uniformity, the Standing Committee of Attorneys-General (SCAG) should adopt an intergovernmental agreement which provides that any proposed changes to the:

(a) model Unified Privacy Principles and relevant definitions used in the *Privacy Act* must be approved by SCAG; and

(b) new *Privacy (Health Information) Regulations* and relevant definitions must be approved by SCAG, in consultation with the Australian Health Ministers' Conference.

The agreement should provide for a procedure whereby the party proposing a change requiring approval must give notice in writing to the other parties to the agreement, and the proposed amendment must be considered and approved by SCAG before being implemented.

**Recommendation 3–6** The Australian Government should initiate a review in five years from the commencement of the amended *Privacy Act* to consider whether the recommended intergovernmental cooperative scheme has been effective in achieving national consistency. This review should consider whether it would be more effective for the Australian Parliament to exercise its legislative power in relation to information privacy to cover the field, including in the state and territory public sectors.

## 5. The *Privacy Act*: Name, Structure and Objects

**Recommendation 5–1** The regulation-making power in the *Privacy Act* should be amended to provide that the Governor-General may make regulations, consistent with the Act, modifying the operation of the model Unified Privacy Principles (UPPs) to impose different or more specific requirements, including

imposing more or less stringent requirements, on agencies and organisations than are provided for in the UPPs.

**Recommendation 5–2** The *Privacy Act* should be redrafted to achieve greater logical consistency, simplicity and clarity.

**Recommendation 5–3** The *Privacy Act* should be renamed the *Privacy and Personal Information Act*. If the *Privacy Act* is amended to incorporate a cause of action for invasion of privacy, however, the name of the Act should remain the same.

**Recommendation 5–4** The *Privacy Act* should be amended to include an objects clause. The objects of the Act should be specified to:

(a) implement, in part, Australia's obligations at international law in relation to privacy;

(b) recognise that individuals have a right to privacy and to promote the protection of that right;

(c) recognise that the right to privacy is not absolute and to provide a framework within which to balance that right with other human rights and to balance the public interest in protecting the privacy of individuals with other public interests;

(d) provide the basis for nationally consistent regulation of privacy and the handling of personal information;

(e) promote the responsible and transparent handling of personal information by agencies and organisations;

(f) facilitate the growth and development of electronic transactions, nationally and internationally, while ensuring respect for the right to privacy;

(g) establish the Australian Privacy Commission and the position of the Privacy Commissioner; and

(h) provide an avenue for individuals to seek redress when there has been an alleged interference with their privacy.

## 6. The *Privacy Act*: Some Important Definitions

**Recommendation 6–1** The *Privacy Act* should define 'personal information' as 'information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified or reasonably identifiable individual'.

**Recommendation 6–2** The Office of the Privacy Commissioner should develop and publish guidance on the meaning of 'identified or reasonably identifiable'.

**Recommendation 6–3** The Office of the Privacy Commissioner should develop and publish guidance on the meaning of 'not reasonably identifiable'.

**Recommendation 6–4** The definition of 'sensitive information' in the *Privacy Act* should be amended to include:

(a) biometric information collected for the purpose of automated biometric verification or identification; and

(b) biometric template information.

**Recommendation 6–5** The definition of 'sensitive information' in the *Privacy Act* should be amended to refer to 'sexual orientation and practices' rather than 'sexual preferences and practices'.

**Recommendation 6–6** The definition of 'record' in the *Privacy Act* should be amended to make clear that a record includes:

(a) a document (as defined in the *Acts Interpretation Act 1901* (Cth)); and

(b) information stored in electronic or other format.

**Recommendation 6–7** The definition of 'generally available publication' in the *Privacy Act* should be amended to clarify that a publication is 'generally available' whether or not a fee is charged for access to the publication.

## 7. Privacy Beyond the Individual

**Recommendation 7–1** The Office of the Privacy Commissioner should encourage and assist agencies and organisations to develop and publish protocols, in consultation with Indigenous groups and representatives, to address the particular privacy needs of Indigenous groups.

**Recommendation 7–2** The Australian Government should undertake an inquiry to consider whether legal recognition and protection of Indigenous cultural rights is required and, if so, the form such recognition and protection should take.

## 8. Privacy of Deceased Individuals

**Recommendation 8–1** The *Privacy Act* should be amended to include provisions dealing with the personal information of individuals who have been dead for 30 years or less where the information is held by an organisation. The Act should provide as follows:

(a) Use and Disclosure

Organisations should be required to comply with the 'Use and Disclosure' principle in relation to the personal information of deceased individuals. Where the principle would have required consent, the organisation should be required to consider whether the proposed use or disclosure would involve an unreasonable use or disclosure of personal information about any person, including the deceased person. The organisation must not use or disclose the information if the use or disclosure would involve an unreasonable use or disclosure of personal information about any person, including the deceased person.

(b) Access

Organisations should be required to provide third parties with access to the personal information of deceased individuals in accordance with the access elements of the 'Access and Correction' principle, except to the extent that providing access would have an unreasonable impact on the privacy of other individuals, including the deceased individual.

(c) Data Quality

Organisations should be required to comply with the use and disclosure elements of the 'Data Quality' principle in relation to the personal information of deceased individuals.

(d) Data Security

Organisations should be required to comply with the 'Data Security' principle in relation to the personal information of deceased individuals.

**Recommendation 8–2** The *Privacy Act* should be amended to provide that the content of National Privacy Principle 2.1(ea) on the use and disclosure of genetic information to genetic relatives—to be moved to the new *Privacy (Health Information) Regulations* in accordance with Recommendation 63–5—should apply to the use and disclosure of genetic information of deceased individuals.

**Recommendation 8–3** Breach of the provisions relating to the personal information of a deceased individual should be considered an interference with privacy under the *Privacy Act*. The following individuals should have standing to lodge a complaint with the Privacy Commissioner:

(a) in relation to an alleged breach of the use and disclosure, access, data quality or data security provisions—the deceased individual's parent, child or sibling who is aged 18 or over, spouse, de facto partner or legal personal representative; and

(b) in relation to an alleged breach of the access provision—the parties in paragraph (a) and any person who has made a request for access to the personal information of a deceased individual where that request has been denied.

# Part B—Developing Technology

## 10. Accommodating Developing Technology in a Regulatory Framework

**Recommendation 10–1** In exercising its research and monitoring functions, the Office of the Privacy Commissioner should consider technologies that can be deployed in a privacy-enhancing way by individuals, agencies and organisations.

**Recommendation 10–2** The Office of the Privacy Commissioner should develop and publish educational materials for individuals, agencies and organisations about specific privacy-enhancing technologies and the privacy-enhancing ways in which technologies can be deployed.

**Recommendation 10–3** The Office of the Privacy Commissioner should develop and publish guidance in relation to technologies that impact on privacy. This guidance should incorporate relevant local and international standards. Matters that such guidance should address include:

(a) developing technologies such as radio frequency identification (RFID) or data-collecting software such as 'cookies';

(b) when the use of a certain technology to collect personal information is not done by 'fair means' and is done 'in an unreasonably intrusive way';

(c) when the use of a certain technology will require agencies and organisations to notify individuals at or before the time of collection of personal information;

(d) when agencies and organisations should notify individuals of certain features of a technology used to collect information (for example, how to remove an RFID tag contained in clothing; or error rates of biometric systems);

(e) the type of information that an agency or organisation should make available to an individual when it is not practicable to provide access to information in an intelligible form (for example, the type of biometric information that is held as a biometric template); and

(f) when it may be appropriate for an agency or organisation to provide human review of a decision made by automated means.

**Recommendation 10–4** The Office of the Privacy Commissioner should develop and publish guidance for organisations on the privacy implications of data-matching.

## 11. Individuals, the Internet and Generally Available Publications

**Recommendation 11–1** The Office of the Privacy Commissioner should develop and publish guidance that relates to generally available publications in an electronic format. This guidance should:

(a) apply whether or not the agency or organisation is required by law to make the personal information publicly available;

(b) set out the factors that agencies and organisations should consider before publishing personal information in an electronic format (for example, whether it is in the public interest to publish on a publicly accessible website personal information about an identified or reasonably identifiable individual); and

(c) clarify the application of the model Unified Privacy Principles to the collection of personal information from generally available publications for inclusion in a record or another generally available publication.

**Recommendation 11–2** The Australian Government should ensure that federal legislative instruments establishing public registers containing personal information set out clearly any restrictions on the electronic publication of that information.

# Part C—Interaction, Inconsistency and Fragmentation

## 14. The Costs of Inconsistency and Fragmentation

**Recommendation 14–1** Agencies that are required or authorised by legislation, a code or a Public Interest Determination to share personal information should, where appropriate, develop and publish documentation that addresses the sharing of personal information; and publish other documents (including memorandums of understanding and ministerial agreements) relating to the sharing of personal information.

**Recommendation 14–2** The Australian Government, in consultation with: state and territory governments; intelligence agencies; law enforcement agencies; and accountability bodies, including the Office of the Privacy Commissioner, the Inspector-General of Intelligence and Security, the Australian Commission for Law Enforcement

Integrity, state and territory privacy commissioners and agencies with responsibility for privacy regulation, and federal, state and territory ombudsmen, should:

(a) develop and publish a framework relating to interjurisdictional sharing of personal information within Australia by intelligence and law enforcement agencies; and

(b) develop memorandums of understanding to clarify the existing roles of accountability bodies that oversee interjurisdictional information sharing within Australia by law enforcement and intelligence agencies.

## 15. Federal Information Laws

**Recommendation 15–1** The *Freedom of Information Act 1982* (Cth) should be amended to provide that disclosure of personal information in accordance with the *Freedom of Information Act* is a disclosure that is required or authorised by or under law for the purposes of the 'Use and Disclosure' principle under the *Privacy Act*.

**Recommendation 15–2** The Australian Government should undertake a review of secrecy provisions in federal legislation. This review should consider, among other matters, how each of these provisions interacts with the *Privacy Act*.

**Recommendation 15–3** Part VIII of the *Privacy Act* (Obligations of confidence) should be repealed.

## 16. Required or Authorised by or Under Law

**Recommendation 16–1** The *Privacy Act* should be amended to provide that 'law', for the purposes of determining when an act or practice is required or authorised by or under law, includes:

(a) Commonwealth, state and territory Acts and delegated legislation;

(b) a duty of confidentiality under common law or equity (including any exceptions to such a duty);

(c) an order of a court or tribunal; and

(d) documents that are given the force of law by an Act, such as industrial awards.

**Recommendation 16–2** The Office of the Privacy Commissioner should develop and publish guidance to clarify when an act or practice will be required or authorised by or under law. This guidance should include:

(a) a list of examples of laws that require or authorise acts or practices in relation to personal information that would otherwise be regulated by the *Privacy Act*; and

(b) a note to the effect that the list is intended to be a guide only and that omission from the list does not mean that a particular law cannot be relied upon for the purposes of a 'required or authorised by or under law' exception in the model Unified Privacy Principles.

**Recommendation 16–3** The Australian Electoral Commission and state and territory electoral commissions, in consultation with the Office of the Privacy Commissioner, state and territory privacy commissioners and agencies with responsibility for privacy regulation, should develop and publish protocols that address the collection, use, storage and destruction of personal information shared for the purposes of the continuous update of the electoral roll.

**Recommendation 16–4** The review under s 251 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) should consider, in particular, whether:

(a) reporting entities and designated agencies are handling personal information appropriately under the legislation;

(b) the number and range of transactions for which identification is required should be more limited than currently provided for under the legislation;

(c) it remains appropriate that reporting entities are required to retain information for seven years;

(d) the use of the electoral roll by reporting entities for the purpose of identification verification is appropriate; and

(e) the handling of information by the Australian Transaction Reports and Analysis Centre is appropriate, particularly as it relates to the provision of access to other bodies, including bodies outside Australia.

## 17. Interaction with State and Territory Laws

**Recommendation 17–1** When an Australian Government agency is participating in an intergovernmental body or other arrangement involving state and territory agencies that handle personal information, the Australian Government agency should ensure that a memorandum of understanding or other arrangement is in place to provide for the appropriate handling of personal information.

**Recommendation 17–2** State and territory privacy legislation should provide for the resolution of complaints by state and territory privacy regulators and agencies with responsibility for privacy regulation in that state or territory's public sector.

**Recommendation 17–3** The Office of the Privacy Commissioner should develop and publish memorandums of understanding with each of the bodies with responsibility for information privacy in Australia, including state and territory bodies and external dispute resolution bodies with responsibility for privacy. These memorandums of understanding should outline:

(a) the roles and functions of each of the bodies;

(b) when a matter will be referred to, or received from, each of the bodies;

(c) processes for consultation between the bodies when issuing Public Interest Determinations and Temporary Public Interest Determinations, approving codes and developing rules; and

(d) processes for developing and publishing joint guidance.

# Part D—The Privacy Principles

## 18. Structural Reform of the Privacy Principles

**Recommendation 18–1** The privacy principles in the *Privacy Act* should be drafted to pursue, as much as practicable, the following objectives:

(a) the obligations in the privacy principles generally should be expressed as high-level principles;

(b) the privacy principles should be technology neutral;

(c) the privacy principles should be simple, clear and easy to understand and apply; and

(d) the privacy principles should impose reasonable obligations on agencies and organisations.

**Recommendation 18–2** The *Privacy Act* should be amended to consolidate the current Information Privacy Principles and National Privacy Principles into a single set of privacy principles, referred to in this Report as the model Unified Privacy Principles.

## 19. Consent

**Recommendation 19–1** The Office of the Privacy Commissioner should develop and publish further guidance about what is required of agencies and organisations to obtain an individual's consent for the purposes of the *Privacy Act*. This guidance should:

(a) address the factors to be taken into account by agencies and organisations in assessing whether consent has been obtained;

(b) cover express and implied consent as it applies in various contexts; and

(c) include advice on when it is and is not appropriate to use the mechanism of 'bundled consent'.

## 20. Anonymity and Pseudonymity

**Recommendation 20–1** The model Unified Privacy Principles should contain a principle called 'Anonymity and Pseudonymity' that requires an agency or organisation to give individuals the clear option to interact anonymously or pseudonymously, where this is lawful and practicable in the circumstances.

**Recommendation 20–2** The Office of the Privacy Commissioner should develop and publish guidance on:

(a) when it is and is not 'lawful and practicable' to give individuals the option to interact anonymously or pseudonymously with agencies or organisations;

(b) what is involved in providing a 'clear option' to interact anonymously or pseudonymously; and

(c) the difference between providing individuals with the option to interact anonymously and pseudonymously.

## 21. Collection

**Recommendation 21–1** The model Unified Privacy Principles should contain a principle called 'Collection' that requires agencies and organisations, where reasonable and practicable, to collect personal information about an individual only from the individual concerned.

**Recommendation 21–2** The Office of the Privacy Commissioner should develop and publish further guidance to clarify when it would not be reasonable and

practicable to collect personal information about an individual only from the individual concerned. In particular, the guidance should address collection:

(a) of personal information by agencies pursuant to the exercise of their coercive information-gathering powers or in accordance with their intelligence-gathering, investigative, and compliance functions;

(b) of statistical data;

(c) of personal information in circumstances in which it is necessary to verify an individual's personal information;

(d) of personal information in circumstances in which the collection process is likely to, or will, disclose the personal information of multiple individuals; and

(e) from persons under the age of 18, persons with a decision-making incapacity and those authorised to provide personal information on behalf of the individual.

**Recommendation 21–3** The 'Collection' principle should provide that, where an agency or organisation receives unsolicited personal information, it must either:

(a) if lawful and reasonable to do so, destroy the information as soon as practicable without using or disclosing it except for the purpose of determining whether the information should be retained; or

(b) comply with all relevant provisions in the model Unified Privacy Principles that apply to the information in question, as if the agency or organisation had taken active steps to collect the information.

**Recommendation 21–4** The Office of the Privacy Commissioner should develop and publish guidance about the meaning of 'unsolicited' in the context of the 'Collection' principle.

**Recommendation 21–5** The 'Collection' principle in the model Unified Privacy Principles should provide that an agency or organisation must not collect personal information unless it is necessary for one or more of its functions or activities.

## 22. Sensitive Information

**Recommendation 22–1** The model Unified Privacy Principles should set out the requirements of agencies and organisations in relation to the collection of personal information that is defined as 'sensitive information' for the purposes of the *Privacy Act*. These requirements should be located in the 'Collection' principle.

**Recommendation 22–2** The sensitive information provisions should contain an exception permitting the collection of sensitive information by an agency or organisation where the collection is required or authorised by or under law.

**Recommendation 22–3** The sensitive information provisions should contain an exception permitting the collection of sensitive information by an agency or organisation where the collection is necessary to lessen or prevent a serious threat to the life or health of any individual, where the individual whom the information concerns is legally or physically incapable of giving or communicating consent.

## 23. Notification

**Recommendation 23–1** The model Unified Privacy Principles should contain a principle called 'Notification' that sets out the requirements on agencies and organisations to notify individuals or otherwise ensure they are aware of particular matters relating to the collection and handling of personal information about the individual.

**Recommendation 23–2** The 'Notification' principle should provide that, at or before the time (or, if that is not practicable, as soon as practicable after) an agency or organisation collects personal information about an individual from the individual or from someone other than the individual, it must take such steps, if any, as are reasonable in the circumstances to notify or otherwise ensure that the individual is aware of the:

(a) fact and circumstances of collection where the individual may not be aware that his or her personal information has been collected;

(b) identity and contact details of the agency or organisation;

(c) rights of access to, and correction of, personal information provided by these principles;

(d) purposes for which the information has been collected;

(e) main consequences of not providing the information;

(f) actual, or types of, agencies, organisations, entities or persons to whom the agency or organisation usually discloses personal information of the kind collected;

(g) fact that the avenues of complaint available to the individual if he or she has a complaint about the collection or handling of his or her personal information are set out in the agency's or organisation's Privacy Policy; and

(h) fact, where applicable, that the collection is required or authorised by or under law.

**Recommendation 23–3** The Office of the Privacy Commissioner should develop and publish guidance to assist agencies and organisations in complying with the 'Notification' principle. In particular, the guidance should address:

(a) the circumstances when it would and would not be reasonable for an agency or organisation to take no steps to notify individuals about the matters specified in the 'Notification' principle. In this regard, the guidance should address the circumstances when:

(i) notification would prejudice the purpose of collection, for example, where it would prejudice:

- the prevention, detection, investigation, and prosecution of offences, breaches of law imposing a penalty or seriously improper conduct;

- the enforcement of laws; or

- the protection of the public revenue;

(ii) the collection of personal information is required or authorised by or under law for statistical or research purposes;

(iii) the personal information is collected from an individual on repeated occasions;

(iv) an individual has been made aware of the relevant matters by the agency or organisation which disclosed the information to the collecting agency or organisation;

(v) non-compliance with the principle is authorised by the individual concerned;

(vi) the taking of no steps is required or authorised by or under law;

(vii) notification would pose a serious threat to the life or health of any individual; and

(viii) health services collect family, social or medical histories;

(b) the appropriate level of specificity when notifying individuals about anticipated disclosures to agencies, organisations, entities and persons; and

(c) the circumstances in which an agency or organisation can comply with specific limbs of the 'Notification' principle by alerting an individual to specific sections of its Privacy Policy or to other general documents.

## 24. Openness

**Recommendation 24–1** The model Unified Privacy Principles should contain a principle called 'Openness'. The principle should set out the requirements on an agency or organisation to operate openly and transparently by setting out clearly expressed policies on its handling of personal information in a Privacy Policy, including how it collects, holds, uses and discloses personal information. This document also should include:

(a) what sort of personal information the agency or organisation holds;

(b) the purposes for which personal information is held;

(c) the steps individuals may take to access and correct personal information about them held by the agency or organisation; and

(d) the avenues of complaint available to individuals in the event that they have a privacy complaint.

**Recommendation 24–2** An agency or organisation should take reasonable steps to make its Privacy Policy, as referred to in the 'Openness' principle, available without charge to an individual electronically; and, on request, in hard copy or in an alternative form accessible to individuals with special needs.

**Recommendation 24–3** The Office of the Privacy Commissioner should continue to encourage and assist agencies and organisations to make available short form privacy notices summarising their personal information-handling practices. Short form privacy notices should be seen as supplementing the more detailed information that is required to be made available to individuals under the *Privacy Act*.

## 25. Use and Disclosure

**Recommendation 25–1** The model Unified Privacy Principles should contain a principle called 'Use and Disclosure' that sets out the requirements on agencies and organisations in respect of the use and disclosure of personal information for a purpose other than the primary purpose of collection.

**Recommendation 25–2** The 'Use and Disclosure' principle should contain an exception permitting an agency or organisation to use or disclose an individual's

personal information for a purpose other than the primary purpose of collection (the secondary purpose), if the:

(a) secondary purpose is related to the primary purpose and, if the personal information is sensitive information, directly related to the primary purpose of collection; and

(b) individual would reasonably expect the agency or organisation to use or disclose the information for the secondary purpose.

**Recommendation 25–3** The 'Use and Disclosure' principle should contain an exception permitting an agency or organisation to use or disclose an individual's personal information for a purpose other than the primary purpose of collection (the secondary purpose) if the agency or organisation reasonably believes that the use or disclosure for the secondary purpose is necessary to lessen or prevent a serious threat to: (a) an individual's life, health or safety; or (b) public health or public safety.

## 26. Direct Marketing

**Recommendation 26–1** The model Unified Privacy Principles should regulate direct marketing by organisations in a discrete privacy principle, separate from the 'Use and Disclosure' principle. This principle should be called 'Direct Marketing' and it should apply regardless of whether the organisation has collected the individual's personal information for the primary purpose or a secondary purpose of direct marketing. The principle should distinguish between direct marketing to individuals who are existing customers and direct marketing to individuals who are not existing customers.

**Recommendation 26–2** The 'Direct Marketing' principle should set out the generally applicable requirements for organisations engaged in the practice of direct marketing. These requirements should be displaced, however, to the extent that more specific sectoral legislation regulates a particular aspect or type of direct marketing.

**Recommendation 26–3** The 'Direct Marketing' principle should provide that an organisation may use or disclose personal information about an individual who is an existing customer aged 15 years or over for the purpose of direct marketing only where the:

(a) individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing; and

(b) organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any direct marketing communications.

**Recommendation 26–4** The 'Direct Marketing' principle should provide that an organisation may use or disclose personal information about an individual who is not an existing customer or is under 15 years of age for the purpose of direct marketing only in the following circumstances:

(a) either:

(i) the individual has consented; or

(ii) the information is not sensitive information and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure;

(b) in each direct marketing communication, the organisation draws to the individual's attention, or prominently displays, a notice advising the individual that he or she may express a wish not to receive any direct marketing communications; and

(c) the organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any direct marketing communications.

**Recommendation 26–5** The 'Direct Marketing' principle should provide that an organisation involved in direct marketing must comply, within a reasonable period of time, with an individual's request not to receive further direct marketing communications and must not charge the individual for giving effect to such a request.

**Recommendation 26–6** The 'Direct Marketing' principle should provide that an organisation that has made direct marketing communications to an individual who is not an existing customer or is under 15 years of age must, where reasonable and practicable and where requested to do so by the individual, advise the individual of the source from which it acquired the individual's personal information.

**Recommendation 26–7** The Office of the Privacy Commissioner should develop and publish guidance to assist organisations in complying with the 'Direct Marketing' principle, including:

(a) what constitutes an 'existing customer';

(b) the types of direct marketing communications which are likely to be within the reasonable expectations of existing customers;

(c) the kinds of circumstances in which it will be impracticable for an organisation to seek consent in relation to direct marketing to an individual who is not an existing customer or is under the age of 15 years;

(d) the factors for an organisation to consider in determining whether it is reasonable and practicable to advise an individual of the source from which it acquired the individual's personal information; and

(e) the obligations of organisations involved in direct marketing under the *Privacy Act* in dealing with vulnerable people.

## 27. Data Quality

**Recommendation 27–1** The model Unified Privacy Principles should contain a principle called 'Data Quality' that requires an agency or organisation to take reasonable steps to make certain that the personal information it collects, uses or discloses is, with reference to the purpose of that collection, use or disclosure, accurate, complete, up-to-date and relevant.

## 28. Data Security

**Recommendation 28–1** The model Unified Privacy Principles should contain a principle called 'Data Security' that applies to agencies and organisations.

**Recommendation 28–2** A note should be inserted after the 'Data Security' principle cross-referencing to the data breach notification provisions.

**Recommendation 28–3** The Office of the Privacy Commissioner should develop and publish guidance about the 'reasonable steps' agencies and organisations should take to prevent the misuse and loss of personal information. This guidance should address matters such as the:

(a) factors that should be taken into account in determining what are 'reasonable steps', including: the likelihood and severity of harm threatened; the sensitivity of the information; the cost of implementation; and any privacy infringements that could result from such data security steps; and

(b) relevant security measures, including privacy-enhancing technologies such as encryption, the security of paper-based and electronic information, and organisational policies and procedures.

**Recommendation 28–4** (a) The 'Data Security' principle should require an agency or organisation to take reasonable steps to destroy or render non-identifiable personal information if:

(i) it is no longer needed for any purpose for which it can be used or disclosed under the model Unified Privacy Principles; and

(ii) retention is not required or authorised by or under law.

(b) The obligation to destroy or render non-identifiable personal information is not 'required by law' for the purposes of s 24 of the *Archives Act 1983* (Cth).

**Recommendation 28–5** The Office of the Privacy Commissioner should develop and publish guidance about the destruction of personal information, or rendering such information non-identifiable. This guidance should address matters such as:

(a) when it is appropriate to destroy or render non-identifiable personal information, including personal information that:

(i) forms part of a historical record; and

(ii) may need to be preserved, in some form, for the purpose of future dispute resolution;

(b) the interaction between the data destruction requirements and legislative records retention requirements; and

(c) the manner in which personal information should be destroyed or rendered non-identifiable.

## 29. Access and Correction

**Recommendation 29–1** The model Unified Privacy Principles should contain a principle called 'Access and Correction' that, subject to Recommendation 29–2, applies consistently to agencies and organisations.

**Recommendation 29–2** The 'Access and Correction' principle should provide that:

(a) if an agency holds personal information about an individual, the individual concerned is entitled to have access to that personal information, except to the extent that the agency is required or authorised to refuse to provide the individual with access to that personal information under the applicable provisions of any law of the Commonwealth that provides for access by persons to documents; and

(b) subject to Recommendation 29–3, if an organisation holds personal information about an individual, the individual concerned shall be entitled to have access to that personal information, except to the extent that one of the exceptions to the right of access presently set out in National Privacy Principle 6.1 or 6.2 applies.

**Recommendation 29–3** The 'Access and Correction' principle should provide that, where an organisation holds personal information about an individual, it is not required to provide access to the information to the extent that providing access would be reasonably likely to pose a serious threat to the life or health of any individual.

**Recommendation 29–4** The 'Access and Correction' principle should provide that, where an agency or organisation is not required to provide an individual with access to his or her personal information, the agency or organisation must take such steps, if any, as are reasonable to provide the individual with as much of the information as possible, including through the use of a mutually agreed intermediary.

**Recommendation 29–5** The 'Access and Correction' principle should provide that, if an individual seeks to have personal information corrected under the principle, an agency or organisation must take such steps, if any, as are reasonable to:

(a) correct the personal information so that, with reference to a purpose for which the information is held, it is accurate, relevant, up-to-date, complete and not misleading; and

(b) notify other entities to whom the personal information has already been disclosed, if requested to do so by the individual and provided such notification would be practicable in the circumstances.

**Recommendation 29–6** The 'Access and Correction' principle should provide that an agency or organisation must, in the following circumstances, if requested to do so by the individual concerned, take reasonable steps to associate with the record a statement of the correction sought:

(a) if the agency or organisation that holds personal information is not willing to correct personal information in accordance with a request by the individual concerned; and

(b) where the personal information is held by an agency, no decision or recommendation to the effect that the record should be amended wholly or partly in accordance with that request has been made under the applicable provisions of a law of the Commonwealth.

**Recommendation 29–7** The 'Access and Correction' principle should provide that an agency or organisation must:

(a) respond within a reasonable period of time to a request from an individual for access to his or her personal information held by the agency or organisation; and

(b) provide access in the manner requested by the individual, where reasonable and practicable.

**Recommendation 29–8** The 'Access and Correction' principle should provide that where an agency or organisation denies a request for access, or refuses to correct personal information, it must provide the individual with:

(a) reasons for the denial of access or refusal to correct personal information, except to the extent that providing such reasons would undermine a lawful reason for denying access or refusing to correct the personal information; and

(b) notice of potential avenues for complaint.

**Recommendation 29–9** The Office of the Privacy Commissioner should develop and publish guidance on the 'Access and Correction' principle, including:

(a) when personal information is 'held' by an agency or organisation;

(b) the requirement that access to personal information should be provided to the maximum extent possible consistent with relevant exceptions;

(c) the factors that an agency or organisation should take into account when determining what is a reasonable period of time to respond to a request for access;

(d) the factors that an agency or organisation should take into account in determining when it would be reasonable and practicable to notify other entities to which it has disclosed personal information of a correction to this information; and

(e) the interrelationships between access to, and correction of, personal information under the *Privacy Act* and other Commonwealth laws, in particular, those relating to freedom of information.

## 30. Identifiers

**Recommendation 30–1** The model Unified Privacy Principles should contain a principle called 'Identifiers' that applies to organisations.

**Recommendation 30–2** The 'Identifiers' principle should include an exception for the adoption, use or disclosure by prescribed organisations of prescribed identifiers in prescribed circumstances. These should be set out in regulations made:

(a) in accordance with the regulation-making mechanism set out in the *Privacy Act*; and

(b) when the Minister is satisfied that the adoption, use or disclosure is for the benefit of the individual concerned.

**Recommendation 30–3** The 'Identifiers' principle should define 'identifier' inclusively to mean a number, symbol or biometric information that is collected for the purpose of automated biometric identification or verification that:

(a) uniquely identifies or verifies the identity of an individual for the purpose of an agency's operations; or

(b) is determined to be an identifier by the Privacy Commissioner.

However, an individual's name or Australian Business Number, as defined in the *A New Tax System (Australian Business Number) Act 1999* (Cth), is not an 'identifier'.

**Recommendation 30–4** The 'Identifiers' principle should contain a note stating that a determination referred to in the 'Identifiers' principle is a legislative instrument for the purposes of s 5 of the *Legislative Instruments Act 2003* (Cth).

**Recommendation 30–5** The 'Identifiers' principle should regulate the adoption, use and disclosure by organisations of identifiers that are assigned by state and territory agencies.

**Recommendation 30–6** Before the introduction by an agency of any multi-purpose identifier, the Australian Government, in consultation with the Privacy Commissioner, should conduct a Privacy Impact Assessment.

**Recommendation 30–7** The Office of the Privacy Commissioner, in consultation with the Australian Taxation Office and other relevant stakeholders, should review the Tax File Number Guidelines issued under s 17 of the *Privacy Act*.

## 31. Cross-border Data Flows

**Recommendation 31–1** (a) The *Privacy Act* should be amended to clarify that it applies to acts done, or practices engaged in, outside Australia by an agency.

(b) The model Unified Privacy Principles should contain a principle called 'Cross-border Data Flows' that applies to agencies and organisations.

**Recommendation 31–2** The 'Cross-border Data Flows' principle should provide that, if an agency or organisation in Australia or an external territory transfers personal information about an individual to a recipient (other than the agency, organisation or the individual) who is outside Australia or an external territory, the agency or organisation remains accountable for that personal information, unless the:

(a) agency or organisation reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds privacy protections that are substantially similar to the model Unified Privacy Principles;

(b) individual consents to the transfer, after being expressly advised that the consequence of providing consent is that the agency or organisation will no longer be accountable for the individual's personal information once transferred; or

(c) agency or organisation is required or authorised by or under law to transfer the personal information.

**Recommendation 31–3** The *Privacy Act* should be amended to provide that 'accountable', for the purposes of the 'Cross-border Data Flows' principle, means that where an agency or organisation transfers personal information to a recipient (other than the agency, organisation or the individual) that is outside Australia or an external territory:

(a) the recipient does an act or engages in a practice outside Australia or an external territory that would have been an interference with the privacy of the individual if done or engaged in within Australia or an external territory; and

(b) the act or practice is an interference with the privacy of the individual, and will be taken to have been an act or practice of the agency or organisation.

**Recommendation 31–4** A note should be inserted after the:

(a) 'Use and Disclosure' principle, cross-referencing to the 'Cross-border Data Flows' principle; and

(b) 'Cross-border Data Flows' principle, cross-referencing to the 'Use and Disclosure' principle.

**Recommendation 31–5** Section 13B of the *Privacy Act* should be amended to clarify that, if an organisation transfers personal information to a related body corporate outside Australia or an external territory, the transfer will be subject to the 'Cross-border Data Flows' principle.

**Recommendation 31–6** The Australian Government should develop and publish a list of laws and binding schemes in force outside Australia that effectively uphold principles for the fair handling of personal information that are substantially similar to the model Unified Privacy Principles.

**Recommendation 31–7** The Office of the Privacy Commissioner should develop and publish guidance on the 'Cross-border Data Flows' principle, including guidance on:

(a) circumstances in which personal information may become available to a foreign government;

(b) outsourcing government services to organisations outside Australia;

(c) the issues that should be addressed as part of a contractual agreement with an overseas recipient of personal information;

(d) what constitutes a 'reasonable belief';

(e) consent to cross-border data flows, including information for individuals on the consequences of providing consent;

(f) the establishment by agencies of administrative arrangements, memorandums of understanding or protocols with foreign governments, with respect to appropriate handling practices for personal information in overseas jurisdictions where privacy protections are not substantially similar to the model Unified Privacy Principles (for example, where the transfer is required or authorised by or under law); and

(g) examples of circumstances which do, and do not, constitute a transfer for the purposes of the 'Cross-border Data Flows' principle.

**Recommendation 31–8** The Privacy Policy of an agency or organisation, referred to in the 'Openness' principle, should set out whether personal information may be transferred outside Australia and the countries to which such information is likely to be transferred.

# Part E—Exemptions

## 33. Overview: Exemptions from the *Privacy Act*

**Recommendation 33–1** The *Privacy Act* should be amended to group together in a separate part of the Act exemptions for certain categories of agencies, organisations and entities or types of acts and practices.

**Recommendation 33–2** The *Privacy Act* should be amended to set out in a schedule to the Act exemptions for specific, named agencies, organisations and entities. The schedule should distinguish between agencies, organisations and entities that are completely exempt and those that are partially exempt from the *Privacy Act*. With respect to partially exempt agencies, organisations and entities, the schedule should specify the particular acts and practices that are exempt.

## 34. Intelligence and Defence Intelligence Agencies

**Recommendation 34–1** (a) The privacy rules and guidelines that relate to the handling of intelligence information concerning Australian persons by the Australian Security Intelligence Organisation, the Australian Secret Intelligence Service, the Defence Imagery and Geospatial Organisation, the Defence Intelligence Organisation, the Defence Signals Directorate and the Office of National Assessments, should be amended to include consistent rules and guidelines relating to:

(i) the handling of personal information about non-Australian individuals, to the extent that this is covered by the *Privacy Act*;

(ii) incidents involving the incorrect use and disclosure of personal information (including a requirement to contact the Inspector-General of Intelligence and Security and advise of incidents and measures taken to protect the privacy of the individual);

(iii) the accuracy of personal information; and

(iv) the storage and security of personal information.

(b) The privacy rules and guidelines should be made available without charge to an individual: electronically on the websites of those agencies; and on request, in hard copy or, where reasonable, in an alternative form accessible to individuals with special needs.

**Recommendation 34–2** Section 15 of the *Intelligence Services Act 2001* (Cth) should be amended to provide that the ministers responsible for the Australian Secret Intelligence Service, the Defence Imagery and Geospatial Organisation, the Defence Signals Directorate and the Defence Intelligence Organisation:

(a) are required to make written rules regulating the handling of intelligence information concerning individuals by the relevant agency, except where:

(i) the agency is engaged in activity outside Australia and the external territories; and

(ii) that activity does not involve the handling of personal information about an Australian citizen or a person whose continued presence in Australia or a territory is not subject to a limitation as to time imposed by law; and

(b) should consult with the relevant agency head, the Privacy Commissioner, the Inspector-General of Intelligence and Security and the minister responsible for administering the *Privacy Act* before making privacy rules about the handling of intelligence information.

**Recommendation 34–3** The *Office of National Assessments Act 1977* (Cth) should be amended to provide that the minister responsible for the Office of National Assessments (ONA):

(a) is required to make written rules regulating the handling of intelligence information about individuals by the ONA, except where:

(i) the ONA is engaged in activity outside Australia and the external territories; and

(ii) that activity does not involve the handling of personal information about an Australian citizen or a person whose continued presence in Australia or a territory is not subject to a limitation as to time imposed by law; and

(b) should consult with the Director-General of the ONA, the Privacy Commissioner, the Inspector-General of Intelligence and Security and the minister responsible for administering the *Privacy Act* before making privacy rules about the handling of intelligence information.

**Recommendation 34–4** Section 8A of the *Australian Security Intelligence Organisation Act 1979* (Cth) should be amended to provide that the:

(a) guidelines issued by the minister responsible for the Australian Security Intelligence Organisation (ASIO) must include guidelines regulating the handling of intelligence information about individuals by ASIO, except where ASIO:

(i) is engaged in activity outside Australia and the external territories; and

(ii) that activity does not involve the handling of personal information about an Australian citizen or a person whose continued presence in Australia or a territory is not subject to a limitation as to time imposed by law; and

(b) minister responsible for ASIO should consult with the Director-General of Security, the Privacy Commissioner, the Inspector-General of Intelligence and Security and the minister responsible for administering the *Privacy Act* before making privacy guidelines about the handling of intelligence information.

**Recommendation 34–5** The *Privacy Act* should be amended to apply to the Inspector-General of Intelligence and Security in respect of the administrative operations of that office.

**Recommendation 34–6** The Inspector-General of Intelligence and Security, in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines in respect of the non-administrative operations of that office.

## 35. Federal Courts and Tribunals

**Recommendation 35–1** The *Privacy Act* should be amended to provide that federal tribunals, boards and commissions whose primary functions involve dispute resolution, administrative review or disciplinary proceedings are exempt from the operation of the Act except in relation to an act done, or a practice engaged in, in respect of a matter of an administrative nature. The schedule to the Act setting out exemptions should list the specific tribunals, boards and commissions that are partially exempt and specify the extent of their exemption.

**Recommendation 35–2** Those federal tribunals, commissions and boards that are partially exempt from the operation of the *Privacy Act* should develop and publish information-handling guidelines that apply to their activities in respect of matters of a non-administrative nature.

**Recommendation 35–3** Federal courts that do not have a policy on granting access for research purposes to court records containing personal information should develop and publish such policies.

## 36. Exempt Agencies under the *Freedom of Information Act*

**Recommendation 36–1** The *Privacy Act* should be amended to remove the partial exemption that applies to the Australian Fair Pay Commission under s 7(1) of the Act.

**Recommendation 36–2** The following agencies listed in Schedule 2, Part I, Division 1 and Part II, Division 1 of the *Freedom of Information Act 1982* (Cth) should be required to demonstrate to the minister responsible for administering the *Privacy Act* that they warrant exemption from the operation of the *Privacy Act*:

(a) Aboriginal Land Councils and Land Trusts;

(b) Auditor-General;

(c) National Workplace Relations Consultative Council;

(d) Department of the Treasury;

(e) Reserve Bank of Australia;

(f) Export and Finance Insurance Corporation;

(g) Australian Communications and Media Authority;

(h) Classification Board;

(i) Classification Review Board; and

(j) Australian Trade Commission.

The Australian Government should remove the exemption from the operation of the *Privacy Act* for any of these agencies that, within 12 months from the tabling of this Report, do not make an adequate case for retaining their exempt status.

**Recommendation 36–3** The *Privacy Act* should be amended to remove the partial exemption that applies to the National Health and Medical Research Council.

**Recommendation 36–4** Subject to the implementation of Recommendation 42–2 (regulations specifying agencies, including the Australian Broadcasting Corporation and the Special Broadcasting Service, as 'media organisations' under the *Privacy Act*), the *Privacy Act* should be amended to remove the partial exemption that applies to the Australian Broadcasting Corporation and the Special Broadcasting Service.

## 37. Agencies with Law Enforcement Functions

**Recommendation 37–1** (a) The Australian Crime Commission (ACC), in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines for the ACC and the Board of the ACC. The information-handling guidelines should address the conditions to be imposed on the recipients of personal information disclosed by the ACC in relation to the further handling of that information.

(b) The Parliamentary Joint Committee on the ACC should monitor compliance by the ACC and the Board of the ACC with the information-handling guidelines.

**Recommendation 37–2** (a) The Integrity Commissioner, in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines for the Integrity Commissioner and the Australian Commission for Law Enforcement Integrity (ACLEI). The information-handling guidelines should address the conditions to be imposed on the recipients of personal information

disclosed by the Integrity Commissioner or the ACLEI in relation to the further handling of that information.

(b) The Internal Audit Committee of the ACLEI and the Parliamentary Joint Committee on the ACLEI should monitor compliance by the Integrity Commissioner and the ACLEI with the information-handling guidelines.

## 38. Other Public Sector Exemptions

**Recommendation 38–1** The Department of the Prime Minister and Cabinet, in consultation with the Office of the Privacy Commissioner, should develop and publish information-handling guidelines for Royal Commissions.

## 39. Small Business Exemption

**Recommendation 39–1** The *Privacy Act* should be amended to remove the small business exemption by:

(a) deleting the reference to 'small business operator' from the definition of 'organisation' in s 6C(1) of the Act; and

(b) repealing ss 6D–6EA of the Act.

**Recommendation 39–2** Before the removal of the small business exemption from the *Privacy Act* comes into effect, the Office of the Privacy Commissioner should provide support to small businesses to assist them in understanding and fulfilling their obligations under the Act, including by:

(a) establishing a national hotline to assist small businesses in complying with the Act;

(b) developing educational materials—including guidelines, information sheets, fact sheets and checklists—on the requirements under the Act;

(c) developing and publishing templates for small businesses to assist in preparing Privacy Policies, to be available electronically and in hard copy free of charge; and

(d) liaising with other Australian Government agencies, state and territory authorities and representative industry bodies to conduct programs to promote an understanding of the privacy principles.

## 40. Employee Records Exemption

**Recommendation 40–1** The *Privacy Act* should be amended to remove the employee records exemption by repealing s 7B(3) of the Act.

**Recommendation 40–2** The Office of the Privacy Commissioner should develop and publish guidance on the application of the model Unified Privacy Principles to employee records, including when it is and is not appropriate to disclose to an employee concerns or complaints by third parties about the employee.

## 41. Political Exemption

**Recommendation 41–1** The *Privacy Act* should be amended to remove the exemption for registered political parties and the exemption for political acts and practices by:

(a) deleting the reference to a 'registered political party' from the definition of 'organisation' in s 6C(1) of the Act;

(b) repealing s 7C of the Act; and

(c) removing the partial exemption that is currently applicable to Australian Government ministers in s 7(1) of the Act.

**Recommendation 41–2** The *Privacy Act* should be amended to provide that the Act does not apply to the extent, if any, that it would infringe any constitutional doctrine of implied freedom of political communication or parliamentary privilege.

**Recommendation 41–3** Parliamentary departments should be included within the definition of 'agency' in the *Privacy Act* by removing the words 'other than the *Privacy Act 1988*' from section 81(1) of the *Parliamentary Services Act 1999* (Cth).

**Recommendation 41–4** Before the removal of the exemptions for registered political parties and for political acts and practices from the *Privacy Act* comes into effect, the Office of the Privacy Commissioner should develop and publish guidance to registered political parties and others to assist them in understanding and fulfilling their obligations under the Act.

## 42. Journalism Exemption

**Recommendation 42–1** The *Privacy Act* should be amended to define 'journalism' to mean the collection, preparation for dissemination or dissemination of the following material for the purpose of making it available to the public:

(a) material having the character of news, current affairs or a documentary;

(b) material consisting of commentary or opinion on, or analysis of, news, current affairs or a documentary; or

(c) material in respect of which the public interest in disclosure outweighs the public interest in maintaining the level of privacy protection afforded by the model Unified Privacy Principles.

**Recommendation 42–2** The definition of 'media organisation' in the *Privacy Act* should be:

(a) amended to 'an organisation whose activities consist of or include journalism'; and

(b) expanded to include an agency that has been specified in the regulations. The regulations should specify, at a minimum, the Australian Broadcasting Corporation and the Special Broadcasting Service.

**Recommendation 42–3** The *Privacy Act* should be amended to provide that media privacy standards must deal *adequately* with privacy in the context of the activities of a media organisation (whether or not the standards also deal with other matters).

**Recommendation 42–4** The Office of the Privacy Commissioner, in consultation with the Australian Communications and Media Authority and peak media representative bodies, should develop and publish:

(a) criteria for adequate media privacy standards; and

(b) a template for media privacy standards that may be adopted by media organisations.

## 44. New Exemptions or Exceptions

**Recommendation 44–1** The *Privacy Act* should be amended to provide an exception to the:

(a) 'Collection' principle to authorise the collection of sensitive information, and

(b) 'Use and Disclosure' principle to authorise the use and disclosure of personal information,

where the collection, use or disclosure by an agency or organisation is necessary for the purpose of a confidential alternative dispute resolution process.

**Recommendation 44–2** The Office of the Privacy Commissioner, in consultation with the National Alternative Dispute Resolution Advisory Council, should develop and publish guidance on what constitutes a confidential alternative dispute resolution process for the purposes of the *Privacy Act*.

**Recommendation 44–3** The Australian Government should recommend that the Council of Australian Governments consider models for the regulation of private investigators and the impact of federal, state and territory privacy laws on their operations.

# Part F—Office of the Privacy Commissioner

## 46. Structure of the Office of the Privacy Commissioner

**Recommendation 46–1** The *Privacy Act* should be amended to change the name of the 'Office of the Privacy Commissioner' to the 'Australian Privacy Commission'.

**Recommendation 46–2** The *Privacy Act* should be amended to provide for the appointment by the Governor-General of one or more Deputy Privacy Commissioners. The Act should provide that, subject to the oversight of the Privacy Commissioner, the Deputy Commissioners may exercise all the powers, duties and functions of the Privacy Commissioner under the Act or any other enactment.

**Recommendation 46–3** The *Privacy Act* should be amended to provide that the Privacy Commissioner must have regard to the objects of the Act, as set out in Recommendation 5–4, in the performance of his or her functions and the exercise of his or her powers.

**Recommendation 46–4** The *Privacy Act* should be amended to make the following changes in relation to the Privacy Advisory Committee:

(a) expand the number of members on the Privacy Advisory Committee, in addition to the Privacy Commissioner, to not more than seven;

(b) require the appointment of a person who has extensive experience in health privacy; and

(c) replace 'electronic data-processing' in s 82(7)(c) with 'information and communication technologies'.

**Recommendation 46–5** The *Privacy Act* should be amended to empower the Privacy Commissioner to establish expert panels, at his or her discretion, to advise the Privacy Commissioner.

## 47. Powers of the Office of the Privacy Commissioner

**Recommendation 47–1** The *Privacy Act* should be amended to delete the word 'computer' from s 27(1)(c).

**Recommendation 47–2** The *Privacy Act* should be amended to reflect that, where guidelines issued or approved by the Privacy Commissioner are binding, they should be renamed 'rules'. For example, the following should be renamed to reflect that a breach of the rules is an interference with privacy under s 13 of the *Privacy Act*:

(a) Tax File Number Guidelines issued under s 17 of the *Privacy Act* should be renamed the *Tax File Number Rules*;

(b) Privacy Guidelines for the Medicare Benefits and Pharmaceutical Benefits Programs (issued under s 135AA of the *National Health Act 1953* (Cth)) should be renamed the *Privacy Rules for the Medicare Benefits and Pharmaceutical Benefits Programs*;

(c) Data-Matching Program (Assistance and Tax) Guidelines (issued under s 12 of the *Data-Matching Program (Assistance and Tax) Act 1990* (Cth)) should be renamed the *Data-Matching Program (Assistance and Tax) Rules*; and

(d) Guidelines on the Disclosure of Genetic Information to a Patient's Genetic Relative should be renamed the *Rules for the Disclosure of Genetic Information to a Patient's Genetic Relative*.

**Recommendation 47–3** Subject to the implementation of Recommendation 24–1, requiring agencies to develop and publish Privacy Policies, the *Privacy Act* should be amended to remove the requirement in s 27(1)(g) to maintain and publish the Personal Information Digest.

**Recommendation 47–4** The *Privacy Act* should be amended to empower the Privacy Commissioner to:

(a) direct an agency to provide to the Privacy Commissioner a Privacy Impact Assessment in relation to a new project or development that the Privacy Commissioner considers may have a significant impact on the handling of personal information; and

(b) report to the ministers responsible for the agency and for administering the *Privacy Act* on the agency's failure to comply with such a direction.

**Recommendation 47–5** The Office of the Privacy Commissioner should develop and publish Privacy Impact Assessment Guidelines tailored to the needs of organisations. A review should be undertaken in five years from the commencement of the amended *Privacy Act* to assess whether the power in Recommendation 47–4 should be extended to include organisations.

**Recommendation 47–6** The *Privacy Act* should be amended to empower the Privacy Commissioner to conduct 'Privacy Performance Assessments' of the records of personal information maintained by organisations for the purpose of ascertaining whether the records are maintained according to the model Unified Privacy Principles, privacy regulations, rules and any privacy code that binds the organisation.

**Recommendation 47–7** The Office of the Privacy Commissioner should publish and maintain on its website a list of all the Privacy Commissioner's functions, including those functions that arise under other legislation.

**Recommendation 47–8** The *Privacy Act* should be amended to empower the Privacy Commissioner to refuse to accept an application for a Public Interest Determination where the Privacy Commissioner is satisfied that the application is frivolous, vexatious or misconceived.

## 48. Privacy Codes

**Recommendation 48–1** Part IIIAA of the *Privacy Act* should be amended to specify that a privacy code:

(a) approved under Part IIIAA operates in addition to the model Unified Privacy Principles (UPPs) and does not replace those principles; and

(b) may provide guidance or standards on how any one or more of the model UPPs should be applied, or are to be complied with, by the organisations bound by the code, as long as such guidance or standards contain obligations that, overall, are at least the equivalent of all the obligations set out in those principles.

## 49. Investigation and Resolution of Privacy Complaints

**Recommendation 49–1** The *Privacy Act* should be amended to provide that, in addition to existing powers not to investigate, the Privacy Commissioner may decide not to investigate, or not to investigate further, an act or practice about which a complaint has been made, or which the Commissioner has accepted under s 40(1B), if the Commissioner is satisfied that:

(a) the complainant has withdrawn the complaint;

(b) the complainant has not responded to the Commissioner for a specified period following a request by the Commissioner for a response in relation to the complaint; or

(c) an investigation, or further investigation, of the act or practice is not warranted having regard to all the circumstances.

**Recommendation 49–2** The *Privacy Act* should be amended to empower the Privacy Commissioner to decline to investigate a complaint where:

(a) the complaint is being handled by an external dispute resolution scheme recognised by the Privacy Commissioner; or

(b) the Privacy Commissioner considers that the complaint would be more suitably handled by an external dispute resolution scheme recognised by the Privacy Commissioner, and should be referred to that scheme.

**Recommendation 49–3** The *Privacy Act* should be amended to empower the Privacy Commissioner to delegate to a state or territory authority all or any of the powers in relation to complaint handling conferred on the Commissioner by the Act.

**Recommendation 49–4** The *Privacy Act* should be amended to clarify the Privacy Commissioner's functions in relation to complaint handling and the process to be followed when a complaint is received.

**Recommendation 49–5** The *Privacy Act* should be amended to include new provisions dealing expressly with conciliation. These provisions should give effect to the following:

(a) If, at any stage after accepting the complaint, the Commissioner considers it reasonably possible that the complaint may be conciliated successfully, he or she must make reasonable attempts to conciliate the complaint.

(b) Where, in the opinion of the Commissioner, reasonable attempts to settle the complaint by conciliation have been made and the Commissioner is satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation, the Commissioner must notify the complainant and respondent that conciliation has failed and the complainant or respondent may require that the complaint be resolved by determination.

(c) Evidence of anything said or done in the course of a conciliation is not admissible in a determination hearing or any enforcement proceedings relating to the complaint, unless all parties to the conciliation otherwise agree.

(d) Subparagraph (c) does not apply where the communication was made in furtherance of the commission of a fraud or an offence, or in the commission of an act that would render a person liable to a civil penalty.

**Recommendation 49–6** The *Privacy Act* should be amended to empower the Privacy Commissioner, in a determination, to prescribe the steps that an agency or respondent must take to ensure compliance with the Act.

**Recommendation 49–7** The *Privacy Act* should be amended to provide that a complainant or respondent can apply to the Administrative Appeals Tribunal for merits review of a determination made by the Privacy Commissioner.

**Recommendation 49–8** The Office of the Privacy Commissioner should develop and publish a document setting out its complaint-handling policies and procedures.

**Recommendation 49–9** The *Privacy Act* should be amended to allow a class member to withdraw from a representative complaint at any time if the class member has not consented to be a class member.

**Recommendation 49–10** The *Privacy Act* should be amended to permit the Privacy Commissioner, in accepting a complaint or determining whether the Commissioner has the power to accept a complaint, to make preliminary inquiries of third parties as well as the respondent. The Privacy Commissioner should be required to inform the complainant that he or she intends to make inquiries of a third party.

**Recommendation 49–11** Section 46(1) of the *Privacy Act* should be amended to empower the Privacy Commissioner to compel parties to a complaint, and any other relevant person, to attend a compulsory conference.

**Recommendation 49–12** The *Privacy Act* should be amended to allow the Privacy Commissioner, in the context of an investigation of a privacy complaint, to collect personal information about an individual who is not the complainant.

**Recommendation 49–13** The *Privacy Act* should be amended to provide that the Privacy Commissioner may direct that a hearing for a determination may be conducted without oral submissions from the parties if the Privacy Commissioner is satisfied that the matter could be determined fairly on the basis of written submissions by the parties.

## 50. Enforcing the *Privacy Act*

**Recommendation 50–1** The *Privacy Act* should be amended to empower the Privacy Commissioner to:

(a) issue a notice to comply to an agency or organisation following an own motion investigation, where the Commissioner determines that the agency or organisation has engaged in conduct constituting an interference with the privacy of an individual;

(b) prescribe in the notice that an agency or organisation must take specified action within a specified period for the purpose of ensuring compliance with the *Privacy Act*; and

(c) commence proceedings in the Federal Court or Federal Magistrates Court for an order to enforce the notice.

**Recommendation 50–2** The *Privacy Act* should be amended to allow the Privacy Commissioner to seek a civil penalty in the Federal Court or Federal Magistrates Court where there is a serious or repeated interference with the privacy of an individual.

**Recommendation 50–3** The Office of the Privacy Commissioner should develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil penalty will be made.

**Recommendation 50–4** The *Privacy Act* should be amended to empower the Privacy Commissioner to accept an undertaking that an agency or organisation will take specified action to ensure compliance with a requirement of the *Privacy Act* or other enactment under which the Commissioner has a power or function. Where an agency or organisation breaches such an undertaking, the Privacy Commissioner may apply to the Federal Court for an order directing the agency or organisation to comply, or any other order the court thinks appropriate.

## 51. Data Breach Notification

**Recommendation 51–1** The *Privacy Act* should be amended to include a new Part on data breach notification, to provide as follows:

(a) An agency or organisation is required to notify the Privacy Commissioner and affected individuals when specified personal information has been, or is reasonably believed to have been, acquired by an unauthorised person and the agency, organisation or Privacy Commissioner believes that the unauthorised acquisition may give rise to a real risk of serious harm to any affected individual.

(b) The definition of 'specified personal information' should include both personal information and sensitive personal information, such as information that combines a person's name and address with a unique identifier, such as a Medicare or account number.

(c) In determining whether the acquisition may give rise to a real risk of serious harm to any affected individual, the following factors should be taken into account:

(i) whether the personal information was encrypted adequately; and

(ii) whether the personal information was acquired in good faith by an employee or agent of the agency or organisation where the agency or organisation was otherwise acting for a purpose permitted by the *Privacy Act* (provided that the personal information is not used or subject to further unauthorised disclosure).

(d) An agency or organisation is not required to notify an affected individual where the Privacy Commissioner considers that notification would not be in the public interest or in the interests of the affected individual.

(e) Failure to notify the Privacy Commissioner of a data breach as required by the Act may attract a civil penalty.

# Part G—Credit Reporting Provisions

## 54. Approach to Reform

**Recommendation 54–1** The credit reporting provisions of the *Privacy Act* should be repealed and credit reporting regulated under the general provisions of the *Privacy Act*, the model Unified Privacy Principles, and regulations under the *Privacy Act*—the new *Privacy (Credit Reporting Information) Regulations*—which impose obligations on credit reporting agencies and credit providers with respect to the handling of credit reporting information.

**Recommendation 54–2** The new *Privacy (Credit Reporting Information) Regulations* should be drafted to contain only those requirements that are different or more specific than provided for in the model Unified Privacy Principles.

**Recommendation 54–3** The new *Privacy (Credit Reporting Information) Regulations* should apply only to 'credit reporting information', defined for the purposes of the new regulations as personal information that is:

(a) maintained by a credit reporting agency in the course of carrying on a credit reporting business; or

(b) held by a credit provider; and

(i) has been prepared by a credit reporting agency; and

(ii) is used, has been used or has the capacity to be used in establishing an individual's eligibility for credit.

**Recommendation 54–4** The new *Privacy (Credit Reporting Information) Regulations* should include a simplified definition of 'credit provider' under which those agencies and organisations that are currently credit providers for the purposes of the *Privacy Act* (whether by operation of s 11B or pursuant to determinations of the Privacy Commissioner) should generally continue to be credit providers for the purposes of the regulations.

**Recommendation 54–5** The new *Privacy (Credit Reporting Information) Regulations* should, subject to Recommendation 54–7, exclude the reporting of personal information about foreign credit and the disclosure of credit reporting information to foreign credit providers.

**Recommendation 54–6** The Australian Government should include credit reporting regulation in the list of areas identified as possible issues for coordination pursuant to the *Memorandum of Understanding Between the Government of New Zealand and the Government of Australia on Coordination of Business Law* (2000).

**Recommendation 54–7** The new *Privacy (Credit Reporting Information) Regulations* should empower the Privacy Commissioner to approve the reporting of personal information about foreign credit, and the disclosure of credit reporting information to foreign credit providers, in defined circumstances. The regulations should set out criteria for approval, including the availability of effective enforcement and complaint handling in the foreign jurisdiction.

**Recommendation 54–8** The Australian Government should, in five years from the commencement of the new *Privacy* (*Credit Reporting Information*) *Regulations*, initiate a review of the regulations.

**Recommendation 54–9** Credit reporting agencies and credit providers, in consultation with consumer groups and regulators, including the Office of the Privacy Commissioner, should develop a credit reporting code providing detailed guidance within the framework provided by the *Privacy Act* and the new *Privacy (Credit Reporting Information) Regulations.* The credit reporting code should deal with a range of operational matters relevant to compliance.

## 55. More Comprehensive Credit Reporting

**Recommendation 55–1** The new *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include the following categories of personal information, in addition to those currently permitted in credit information files under the *Privacy Act*:

(a) the type of each credit account opened (for example, mortgage, personal loan, credit card);

(b) the date on which each credit account was opened;

(c) the current limit of each open credit account; and

(d) the date on which each credit account was closed.

**Recommendation 55–2** Subject to Recommendation 55–3, the new *Privacy (Credit Reporting Information) Regulations* should also permit credit reporting information to include an individual's repayment performance history, comprised of information indicating:

(a) whether, over the prior two years, the individual was meeting his or her repayment obligations as at each point of the relevant repayment cycle for a credit account; and, if not,

(b) the number of repayment cycles the individual was in arrears.

**Recommendation 55–3** The Australian Government should implement Recommendation 55–2 only after it is satisfied that there is an adequate framework imposing responsible lending obligations in Commonwealth, state and territory legislation.

**Recommendation 55–4** The credit reporting code should set out procedures for reporting repayment performance history, within the parameters prescribed by the new *Privacy (Credit Reporting Information) Regulations*.

**Recommendation 55–5** The new Privacy *(Credit Reporting Information) Regulations* should provide for the deletion of the information referred to in Recommendation 55–1 two years after the date on which a credit account is closed.

## 56. Collection and Permitted Content of Credit Reporting Information

**Recommendation 56–1** The new *Privacy (Credit Reporting Information) Regulations* should prescribe an exhaustive list of the categories of personal information that are permitted to be included in credit reporting information. This list

should be based on the provisions of s 18E of the *Privacy Act*, subject to the changes set out in Recommendations 55–1, 55–2, 56–2 to 56–4, 56–6, 56–8 and 56–9.

**Recommendation 56–2** The new *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies are not permitted to list overdue payments of less than a prescribed amount.

**Recommendation 56–3** The new *Privacy (Credit Reporting Information) Regulations* should not permit credit reporting information to include information about presented and dishonoured cheques.

**Recommendation 56–4** The new *Privacy (Credit Reporting Information) Regulations* should permit credit reporting information to include personal insolvency information recorded on the National Personal Insolvency Index administered under the *Bankruptcy Regulations 1966* (Cth).

**Recommendation 56–5** Credit reporting agencies should ensure that credit reports adequately differentiate the forms of administration identified on the National Personal Insolvency Index (NPII); and accurately reflect the relevant information recorded on the NPII, as updated from time to time.

**Recommendation 56–6** The new *Privacy (Credit Reporting Information) Regulations* should allow for the listing of a 'serious credit infringement' based on the definition currently set out in s 18E(1)(b)(x) of the *Privacy Act*, amended so that the credit provider is required to have taken reasonable steps to contact the individual before reporting a serious credit infringement under s 18E(1)(b)(x)(c).

**Recommendation 56–7** The Office of the Privacy Commissioner should develop and publish guidance on the criteria that need to be satisfied before a serious credit infringement may be listed, including:

(a) how to interpret 'serious' (for example, in terms of the individual's conduct, and the period and amount of overdue payments);

(b) how to establish whether reasonable steps to contact the individual have been taken;

(c) whether a serious credit infringement should be listed where there is a dispute between the parties that is subject to dispute resolution; and

(d) the obligations on credit providers and individuals in proving or disproving that a serious credit infringement has occurred.

**Recommendation 56–8** The new *Privacy (Credit Reporting Information) Regulations* should prohibit the collection in credit reporting information of 'sensitive information', as defined in the *Privacy Act*.

**Recommendation 56–9** The new *Privacy (Credit Reporting Information) Regulations* should prohibit the collection of credit reporting information about individuals who the credit provider or credit reporting agency knows, or reasonably should know, to be under the age of 18.

**Recommendation 56–10** The new *Privacy (Credit Reporting Information) Regulations* should provide, in addition to the other provisions of the 'Notification' principle, that at or before the time personal information to be disclosed to a credit reporting agency is collected about an individual, a credit provider must take such steps as are reasonable, if any, to ensure that the individual is aware of the:

(a) identity and contact details of the credit reporting agency;

(b) rights of access to, and correction of, credit reporting information provided by the regulations; and

(c) actual or types of organisations, agencies, entities or persons to whom the credit reporting agency usually discloses credit reporting information.

**Recommendation 56–11** The new *Privacy (Credit Reporting Information) Regulations* should provide that a credit provider, before disclosing overdue payment information to a credit reporting agency, must have taken reasonable steps to ensure that the individual concerned is aware of the intention to report the information. Overdue payment information, for these purposes, means the information currently referred to in s 18E(b)(1)(vi) of the *Privacy Act.*

## 57. Use and Disclosure of Credit Reporting Information

**Recommendation 57–1** The new *Privacy (Credit Reporting Information) Regulations* should provide a simplified list of circumstances in which a credit reporting agency or credit provider may use or disclose credit reporting information. This list should be based on the provisions of Part IIIA of the *Privacy Act*, which currently authorise the use and disclosure by credit reporting agencies and credit providers of personal information contained in credit information files, credit reports and reports relating to credit worthiness (ss 18L, 18K and 18N).

**Recommendation 57–2** The new *Privacy (Credit Reporting Information) Regulations* should provide that a credit reporting agency or credit provider may use or disclose credit reporting information for a secondary purpose related to the assessment of an application for credit or the management of an existing credit account, where the individual concerned would reasonably expect such use or disclosure.

**Recommendation 57–3** The new *Privacy (Credit Reporting Information) Regulations* should prohibit the use or disclosure of credit reporting information for the purposes of direct marketing, including the pre-screening of direct marketing lists.

**Recommendation 57–4** The use and disclosure of credit reporting information for electronic identity verification purposes to satisfy obligations under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth) (AML/CTF Act) should be authorised expressly under the AML/CTF Act.

**Recommendation 57–5** The new *Privacy (Credit Reporting Information) Regulations* should provide individuals with a right to prohibit for a specified period the disclosure by a credit reporting agency of credit reporting information about them without their express authorisation.

**Recommendation 57–6** There should be no equivalent in the new *Privacy (Credit Reporting Information) Regulations* of s 18N of the *Privacy Act*, which limits the disclosure by credit providers of personal information in 'reports' related to credit worthiness. The use and disclosure limitations should apply only to 'credit reporting information' as defined for the purposes of the new regulations.

## 58. Data Quality and Security

**Recommendation 58–1** The new *Privacy (Credit Reporting Information) Regulations* should prohibit expressly the listing of any overdue payment where the credit provider is prevented under any law of the Commonwealth, a state or a territory from bringing proceedings against the individual to recover the amount of the overdue payment; or where any relevant statutory limitation period has expired.

**Recommendation 58–2** The new *Privacy (Credit Reporting Information) Regulations* should provide that where the individual has entered into a new arrangement with a credit provider to repay an existing debt—such as by entering into a scheme of arrangement with the credit provider—an overdue payment under the new arrangement may be listed and remain part of the individual's credit reporting information for the full five-year period permissible under the regulations.

**Recommendation 58–3** The credit reporting code should promote data quality by setting out procedures to ensure consistency and accuracy of credit reporting information. These procedures should deal with matters including:

(a) the timeliness of the reporting of credit reporting information;

(b) the calculation of overdue payments for credit reporting purposes;

(c) obligations to prevent the multiple listing of the same debt;

(d) the updating of credit reporting information; and

(e) the linking of credit reporting information relating to individuals who may or may not be the same individual.

**Recommendation 58–4** The new *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies must:

(a) enter into agreements with credit providers that contain obligations to ensure the quality and security of credit reporting information;

(b) establish and maintain controls to ensure that only credit reporting information that is accurate, complete and up-to-date is used or disclosed;

(c) monitor data quality and audit compliance with the agreements and controls; and

(d) identify and investigate possible breaches of the agreements and controls.

**Recommendation 58–5** The new *Privacy (Credit Reporting Information) Regulations* should provide for the deletion by credit reporting agencies of different categories of credit reporting information after the expiry of maximum permissible periods, based on those currently set out in s 18F of the *Privacy Act*.

**Recommendation 58–6** The new *Privacy (Credit Reporting Information) Regulations* should provide for the deletion by credit reporting agencies of information about voluntary arrangements with creditors under Parts IX and X of the *Bankruptcy Act 1966* (Cth) five years from the date of the arrangement as recorded on the National Personal Insolvency Index.

## 59. Access and Correction, Complaint Handling and Penalties

**Recommendation 59–1** The new *Privacy (Credit Reporting Information) Regulations* should provide individuals with a right to obtain access to credit reporting information based on the provisions currently set out in s 18H of the *Privacy Act*.

**Recommendation 59–2** The new *Privacy (Credit Reporting Information) Regulations* should provide that credit reporting agencies must provide individuals, on request, with one free copy of their credit reporting information annually.

**Recommendation 59–3** The new *Privacy (Credit Reporting Information) Regulations* should provide an equivalent of s 18H(3) of the *Privacy Act*, so that an individual's rights of access to credit reporting information may be exercised for a credit-related purpose by a person authorised in writing.

**Recommendation 59–4** The new *Privacy (Credit Reporting Information) Regulations* should provide that, where a credit provider refuses an application for credit based wholly or partly on credit reporting information, it must notify an individual of that fact. These notification requirements should be based on the provisions currently set out in s 18M of the *Privacy Act*.

**Recommendation 59–5** The new *Privacy (Credit Reporting Information) Regulations* should provide that:

(a) credit reporting agencies and credit providers must establish procedures to deal with a request by an individual for resolution of a credit reporting complaint in a fair, efficient and timely manner;

(b) a credit reporting agency should refer to a credit provider for resolution complaints about the content of credit reporting information provided to the agency by that credit provider; and

(c) where a credit reporting agency or credit provider establishes that it is unable to resolve a complaint, it must inform the individual concerned that it is unable to resolve the complaint and that the individual may complain to an external dispute resolution scheme or to the Privacy Commissioner.

**Recommendation 59–6** The new *Privacy (Credit Reporting Information) Regulations* should provide that the information to be given, if an individual's application for credit is refused based wholly or partly on credit reporting information, should include the avenues of complaint available to the individual if he or she has a complaint about the content of his or her credit reporting information.

**Recommendation 59–7** The new *Privacy (Credit Reporting Information) Regulations* should provide that credit providers only may list overdue payment or repayment performance history where the credit provider is a member of an external dispute resolution scheme recognised by the Privacy Commissioner.

**Recommendation 59–8** The new *Privacy (Credit Reporting Information) Regulations* should provide that, within 30 days, evidence to substantiate disputed credit reporting information must be provided to the individual, or the matter referred to an external dispute resolution scheme recognised by the Privacy Commissioner. If these requirements are not met, the credit reporting agency must delete or correct the information on the request of the individual concerned.

**Recommendation 59–9** The *Privacy Act* should be amended to remove the credit reporting offences and allow a civil penalty to be imposed as provided for by Recommendation 50–2.

# Part H—Health Services and Research

## 60. Regulatory Framework for Health Information

**Recommendation 60–1** Health information should be regulated under the general provisions of the *Privacy Act*, the model Unified Privacy Principles (UPPs), and regulations under the *Privacy Act*—the new *Privacy (Health Information) Regulations*. The new *Privacy (Health Information) Regulations* should be drafted to contain only those requirements that are different or more specific than provided for in the model UPPs.

**Recommendation 60–2** The Office of the Privacy Commissioner should publish a document bringing together the model Unified Privacy Principles (UPPs) and the additions set out in the new *Privacy (Health Information) Regulations*. This document should contain a complete set of the model UPPs as they relate to health information.

**Recommendation 60–3** The Office of the Privacy Commissioner—in consultation with the Department of Health and Ageing and other relevant stakeholders—should develop and publish guidelines on the handling of health information under the *Privacy Act* and the new *Privacy (Health Information) Regulations*.

## 61. Electronic Health Information Systems

**Recommendation 61–1** If a national Unique Healthcare Identifiers (UHIs) or a national Shared Electronic Health Records (SEHR) scheme goes forward, it should be established under specific enabling legislation. This legislation should address information privacy issues, such as:

(a) the nomination of an agency or organisation with clear responsibility for managing the respective systems, including the personal information contained in the systems;

(b) the eligibility criteria, rights and requirements for participation in the UHI and SEHR schemes by health consumers and health service providers, including consent requirements;

(c) permitted and prohibited uses and linkages of the personal information held in the systems;

(d) permitted and prohibited uses of UHIs and sanctions in relation to misuse; and

(e) safeguards in relation to the use of UHIs, including providing that it is not necessary to use a UHI in order to access health services.

## 62. The *Privacy Act* and Health Information

**Recommendation 62–1** The definition of 'health information' in the *Privacy Act* should be amended to make express reference to the *physical, mental or psychological* health or disability of an individual.

**Recommendation 62–2** The *Privacy Act* should be amended to define a 'health service' as:

(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the service provider to:

  (i) assess, predict, maintain or improve the individual's physical, mental or psychological health or status;

  (ii) diagnose the individual's illness, injury or disability; or

  (iii) prevent or treat the individual's illness, injury or disability or suspected illness, injury or disability;

(b) a health-related disability, palliative care or aged care service;

(c) a surgical or related service; or

(d) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

## 63. *Privacy (Health Information) Regulations*

**Recommendation 63–1** The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Collection' principle, an agency or organisation that provides a health service may collect health information from an individual, or a person responsible for the individual, about third parties when:

(a) the collection of the third party's information is necessary to enable the health service provider to provide a health service directly to the individual; and

(b) the third party's information is relevant to the family, social or medical history of that individual.

**Recommendation 63–2** The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Collection' principle, an agency or organisation that is a health service provider may collect health information about an individual if the information is necessary to provide a health service to the individual and the individual would reasonably expect the agency or organisation to collect the information for that purpose.

**Recommendation 63–3** National Privacy Principles (NPPs) 2.4 to 2.6—dealing with the disclosure of health information by a health service provider to a person who is responsible for an individual—should be moved to the new *Privacy (Health Information) Regulations*. The new regulations should provide that, in addition to the other provisions of the 'Use and Disclosure' principle, an agency or organisation that provides a health service to an individual may disclose health information about the individual to a person who is responsible for the individual, if the individual is incapable of giving consent to the disclosure and all the other circumstances currently set out in NPP 2.4 are met. In addition, the new regulations should:

(a) be expressed to apply to both agencies and organisations;

(b) not refer to a health service provider who may make a disclosure under these provisions as a 'carer'; and

(c) define 'a person who is responsible for an individual' as:

  (i) a parent, child or sibling of the individual;

  (ii) a spouse or de facto partner of the individual;

  (iii) a relative of the individual who is a member of the individual's household;

  (iv) a substitute decision maker authorised by a federal, state or territory law to make decisions about the individual's health;

  (v) a person who has an intimate personal relationship with the individual;

  (vi) a person nominated by the individual to be contacted in case of emergency; or

  (vii) a person who is primarily responsible for providing support or care to the individual.

In considering whether to disclose an individual's health information to a person who is responsible for an individual and who is under the age of 18, a health service provider should consider, on a case-by-case basis, that person's maturity and capacity to understand the information.

**Recommendation 63–4** The *Privacy Act* should be amended to provide a definition of 'de facto partner' in the following terms: 'de facto partner' means a person in a relationship as a couple with another person to whom he or she is not married.

**Recommendation 63–5** The new *Privacy (Health Information) Regulations* should include provisions similar to those set out in National Privacy Principle 2.1(ea) on the use and disclosure of genetic information where necessary to lessen or prevent a serious threat to the life, health or safety of a genetic relative. These regulations should apply to both agencies and organisations. Any use or disclosure under the new regulations should be in accordance with rules issued by the Privacy Commissioner.

**Recommendation 63–6** The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Access and Correction' principle, if an individual is denied access to his or her own health information by an agency on the basis that providing access would, or could reasonably be expected to, endanger the life or physical safety of any person, or by an organisation on the basis that providing access would be reasonably likely to pose a serious threat to the life or health of any individual:

(a) the agency or organisation must advise the individual that he or she may nominate a suitably qualified health service provider ('nominated health service provider') to be given access to the health information;

(b) the individual may nominate a health service provider and request that the agency or organisation provide the nominated health service provider with access to the information;

(c) if the agency or organisation does not object to the nominated health service provider, it must provide the nominated health service provider with access to the health information within a reasonable period of time; and

(d) the nominated health service provider may assess the grounds for denying access to the health information and may provide the individual with access to the information to the extent that the nominated health service provider is satisfied that to do so, in the case of an agency, would not, or could not be reasonably expected to, endanger the life or physical safety of any person and, in the case of an organisation, would not be reasonably likely to pose a serious threat to the life or health of any individual.

If the agency or organisation objects to the nominated health service provider and refuses to provide the nominated health service provider with access to the information, the individual may nominate another suitably qualified health service provider, or may lodge a complaint with the Privacy Commissioner alleging an interference with privacy.

**Recommendation 63–7** The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Data Security' principle, where an agency or organisation that provides a health service is sold, amalgamated or closed down, and an individual health service provider will not be providing health services in the new agency or organisation, or an individual health service provider dies, the provider, or the legal representative of the provider, must take reasonable steps to:

(a) make individual users of the health service aware of the sale, amalgamation or closure of the health service, or the death of the health service provider; and

(b) inform individual users of the health service about proposed arrangements for the transfer or storage of individuals' health information.

**Recommendation 63–8** (a) The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Access and Correction' principle, where an individual requests that an agency or organisation that is a health service provider transfers the individual's health information to another health service provider, the agency or organisation must respond within a reasonable time and transfer the information.

(b) Other elements of the 'Access and Correction' principle relating to access should apply to a request for transfer from one health service provider to another, amended as necessary.

**Recommendation 63–9** The new *Privacy (Health Information) Regulations* should provide that, in addition to the other provisions of the 'Collection' principle and the 'Use and Disclosure' principle, an agency or organisation may collect, use or disclose health information where necessary for the funding, management, planning, monitoring, or evaluation of a health service where:

(a) the purpose cannot be achieved by the collection, use or disclosure of information that does not identify the individual or from which the individual would not be reasonably identifiable;

(b) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent before the collection, use or disclosure; and

(c) the collection, use or disclosure is conducted in accordance with rules issued by the Privacy Commissioner.

**Recommendation 63–10** The *Privacy Act* should be amended to empower the Privacy Commissioner to issue rules in relation to the handling of personal information for the funding, management, planning, monitoring, or evaluation of a health service.

## 65. Research: Recommendations for Reform

**Recommendation 65–1** (a) The Privacy Commissioner should issue one set of rules under the research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle to replace the *Guidelines under Section 95 of the Privacy Act 1988* and the *Guidelines Approved under Section 95A of the Privacy Act 1988*.

(b) The Privacy Commissioner should consult with relevant stakeholders in developing the rules to be issued under the research exceptions to the 'Collection' and 'Use and Disclosure' principles—that is, the 'Research Rules'.

(c) Those elements of the *National Statement on Ethical Conduct in Human Research* dealing with privacy should be aligned with the *Privacy Act* and the Research Rules to minimise confusion for institutions, researchers and Human Research Ethics Committees.

**Recommendation 65–2** The *Privacy Act* should be amended to extend the arrangements relating to the collection, use or disclosure of personal information without consent in the area of health and medical research to cover the collection, use or disclosure of personal information without consent in human research more generally.

**Recommendation 65–3** The *Privacy Act* should be amended to provide that 'research' includes the compilation or analysis of statistics.

**Recommendation 65–4** The research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle should provide that, before approving an activity that involves the collection, use or disclosure of sensitive information or the use or disclosure of other personal information without consent, Human Research Ethics Committees must be satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*.

**Recommendation 65–5** The research exceptions to the 'Collection' principle and the 'Use and Disclosure' principle should include a provision stating that it must be 'unreasonable or impracticable' to seek consent from individuals to the collection, use or disclosure of their personal information before that information may be used without consent for the purposes of research.

**Recommendation 65–6** The National Health and Medical Research Council, the Australian Research Council and Universities Australia should amend the *National Statement on Ethical Conduct in Human Research* to state that, where a research proposal seeks to rely on the research exceptions in the *Privacy Act*, it must be reviewed and approved by a Human Research Ethics Committee.

**Recommendation 65–7** The Privacy Commissioner, in consultation with relevant stakeholders, should review the reporting requirements imposed under the *Privacy Act* on the Australian Health Ethics Committee and Human Research Ethics Committees. Any new reporting mechanism should aim to promote the objects of the *Privacy Act*, have clear goals and impose the minimum possible administrative burden to achieve those goals.

**Recommendation 65–8** The research exception to the 'Collection' principle should provide that an agency or organisation may collect personal information, including sensitive information, about an individual where all of the following conditions are met:

(a) the collection is necessary for research;

(b) the purpose cannot be served by the collection of information that does not identify the individual;

(c) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the collection;

(d) a Human Research Ethics Committee—constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research* as in force from time to time—has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*; and

(e) the information is collected in accordance with the Research Rules, to be issued by the Privacy Commissioner.

Where an agency or organisation collects personal information about an individual under this exception, it must take reasonable steps to ensure that the information is not disclosed in a form that would identify the individual or from which the individual would be reasonably identifiable.

**Recommendation 65–9** The research exception to the 'Use and Disclosure' principle should provide that an agency or organisation may use or disclose personal information where all of the following conditions are met:

(a) the use or disclosure is necessary for research;

(b) it is unreasonable or impracticable for the agency or organisation to seek the individual's consent to the use or disclosure;

(c) a Human Research Ethics Committee—constituted in accordance with, and acting in compliance with, the *National Statement on Ethical Conduct in Human Research* as in force from time to time—has reviewed the proposed activity and is satisfied that the public interest in the activity outweighs the public interest in maintaining the level of privacy protection provided by the *Privacy Act*;

(d) the information is used or disclosed in accordance with the Research Rules, to be issued by the Privacy Commissioner; and

(e) in the case of disclosure—the agency or organisation reasonably believes that the recipient of the personal information will not disclose the information in a form that would identify the individual or from which the individual would be reasonably identifiable.

## 66. Research: Databases and Data Linkage

**Recommendation 66–1** The Privacy Commissioner should address the following matters in the Research Rules:

(a) in what circumstances and under what conditions it is appropriate to collect, use or disclose personal information without consent for inclusion in a database or register for research purposes; and

(b) the fact that, where a database or register is established on the basis of Human Research Ethics Committee approval, that approval does not extend to future unspecified uses. Any future proposed use of the database or register for research would require separate review by a Human Research Ethics Committee.

**Recommendation 66–2** Agencies or organisations developing systems or infrastructure to allow the linkage of personal information for research purposes should conduct a Privacy Impact Assessment to ensure that the privacy risks involved are assessed and adequately managed in the design and implementation of the project.

**Recommendation 66–3** The Research Rules, to be issued by the Privacy Commissioner, should address the circumstances in which, and the conditions under which, it is appropriate to collect, use or disclose personal information without consent in order to identify potential participants in research.

# Part I—Children, Young People and Adults Requiring Assistance

## 67. Children, Young People and Attitudes to Privacy

**Recommendation 67–1** The Australian Government should fund a longitudinal study of the attitudes of Australians, in particular young Australians, to privacy.

**Recommendation 67–2** The Office of the Privacy Commissioner should develop and publish educational material about privacy issues aimed at children and young people.

**Recommendation 67–3** The Office of the Privacy Commissioner, in consultation with the Australian Communications and Media Authority, should ensure that specific guidance on the privacy aspects of using social networking websites is developed and incorporated into publicly available educational material.

**Recommendation 67–4** In order to promote awareness of personal privacy and respect for the privacy of others, state and territory education departments should incorporate education about privacy, including privacy in the online environment, into school curriculums.

## 68. Decision Making by and for Individuals Under the Age of 18

**Recommendation 68–1** The *Privacy Act* should be amended to provide that where it is reasonable and practicable to make an assessment about the capacity of an individual under the age of 18 to give consent, make a request or exercise a right of access under the Act, an assessment about the individual's capacity should be undertaken. Where an assessment of capacity is not reasonable or practicable, then an individual:

(a) aged 15 or over is presumed to be capable of giving consent, making a request or exercising a right of access; and

(b) under the age of 15 is presumed to be incapable of giving consent, making a request or exercising a right of access.

**Recommendation 68–2** The *Privacy Act* should be amended to provide that where an individual under the age of 18 is assessed or presumed to not have capacity under the Act, any consent, request or exercise of a right in relation to that individual must be provided or made by a person with parental responsibility for the individual.

**Recommendation 68–3** The *Privacy Act* should be amended to provide that, in order to rely on the age-based presumption, an agency or organisation is required to take such steps, if any, as are reasonable in the circumstances to verify that the individual is aged 15 or over.

**Recommendation 68–4** The Office of the Privacy Commissioner should develop and publish guidance for applying the new provisions of the *Privacy Act* relating to individuals under the age of 18, including on:

(a) the involvement of children, young people and persons with parental responsibility in decision-making processes;

(b) situations in which it is reasonable and practicable to make an assessment regarding capacity of children and young people;

(c) practices and criteria to be used in determining whether a child or young person is capable of giving consent, making a request or exercising a right on his or her own behalf, including reasonable steps required to verify the age of an individual;

(d) the provision of reasonable assistance to children and young people to understand and communicate decisions; and

(e) the requirements to obtain consent from a person with parental responsibility for the child or young person in appropriate circumstances.

**Recommendation 68–5** Agencies and organisations that regularly handle the personal information of individuals under the age of 18 should address in their Privacy Policies how such information is managed and how the agency or organisation will determine the capacity of individuals under the age of 18.

**Recommendation 68–6** Agencies and organisations that regularly handle the personal information of individuals under the age of 18 should ensure that relevant staff receive training about issues concerning capacity, including when it is necessary to deal with third parties on behalf of those individuals.

## 69. Particular Privacy Issues Affecting Children and Young People

**Recommendation 69–1** Schools subject to the *Privacy Act* should clarify in their Privacy Policies how the personal information of students will be handled, including when personal information:

(a) will be disclosed to, or withheld from, persons with parental responsibility and other representatives; and

(b) collected by school counsellors will be disclosed to school management, persons with parental responsibility, or others.

**Recommendation 69–2** The Ministerial Council on Education, Employment, Training and Youth Affairs should consider the handling of personal information in schools, with a view to developing uniform policies across the states and territories consistent with the *Privacy Act*.

## 70. Third Party Representatives

**Recommendation 70–1** The *Privacy Act* should be amended to include the concept of a 'nominee' and provide that an agency or organisation may establish nominee arrangements. The agency or organisation should then deal with an individual's nominee as if the nominee were the individual.

**Recommendation 70–2** The *Privacy Act* should be amended to provide for nominee arrangements, which should include, at a minimum, the following elements:

(a) a nomination can be made by an individual or a substitute decision maker authorised by a federal, state or territory law;

(b) the nominee can be an individual or an entity;

(c) the nominee has a duty to act at all times in the best interests of the individual; and

(d) the nomination can be revoked by the individual, the nominee or the agency or organisation.

**Recommendation 70–3** The Office of the Privacy Commissioner should develop and publish guidance for dealing with third party representatives, including in relation to:

(a) the involvement of third parties, with the consent of an individual, to assist the individual to make and communicate privacy decisions;

(b) establishing and administering nominee arrangements;

(c) identifying and dealing with issues concerning capacity; and

(d) recognising and verifying the authority of substitute decision makers authorised by a federal, state or territory law.

**Recommendation 70–4** Agencies and organisations that regularly handle personal information about adults with limited or no capacity to provide consent, make a request or exercise a right under the *Privacy Act*, should ensure that relevant staff are trained adequately in relation to issues concerning capacity, and in recognising and verifying the authority of third party representatives.

# Part J—Telecommunications

## 71. *Telecommunications Act*

**Recommendation 71–1** Part 13 of the *Telecommunications Act 1997* (Cth) should be redrafted to achieve greater logical consistency, simplicity and clarity.

**Recommendation 71–2** The Australian Government should initiate a review to consider whether the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth) continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and changing community perceptions and expectations about communication technologies. In particular, the review should consider:

(a) whether the Acts continue to regulate effectively communication technologies and the individuals and organisations that supply communication technologies and communication services;

(b) how these two Acts interact with each other and with other legislation;

(c) the extent to which the activities regulated under the Acts should be regulated under general communications legislation or other legislation;

(d) the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry, including the Australian Communications and Media Authority, the Attorney-General's Department, the Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman, and Communications Alliance; and

(e) whether the *Telecommunications (Interception and Access) Act* should be amended to provide for the role of a public interest monitor.

**Recommendation 71–3** The *Telecommunications Act 1997* (Cth) should be amended to provide that a breach of Divisions 2, 4 and 5 of Part 13 of the Act may attract a civil penalty in addition to a criminal penalty. The Australian Communications and Media Authority should develop and publish enforcement guidelines setting out the criteria upon which a decision to pursue a civil or a criminal penalty is made.

**Recommendation 71–4** The Australian Communications and Media Authority, in consultation with the Office of the Privacy Commissioner, Communications Alliance, the Telecommunications Industry Ombudsman, and other relevant stakeholders, should develop and publish guidance that addresses privacy issues raised by new technologies such as location-based services, voice over internet protocol and electronic number mapping.

**Recommendation 71–5** Section 117(1)(k) of the *Telecommunications Act 1997* (Cth) should be amended to provide that the Australian Communications and Media Authority cannot register a code that deals directly or indirectly with a matter dealt with by the *Privacy Act*, or an approved privacy code under the *Privacy Act*, unless it has consulted with, and taken into consideration any comments or suggested amendments of, the Privacy Commissioner.

**Recommendation 71–6** Section 134 of the *Telecommunications Act 1997* (Cth) should be amended to provide that the Australian Communications and Media Authority cannot determine or vary an industry standard that deals directly or indirectly with a matter dealt with by the *Privacy Act*, or an approved privacy code under the *Privacy Act*, unless it has consulted with, and taken into consideration any comments or suggested amendments of, the Privacy Commissioner.

## 72. Exceptions to the Use and Disclosure Offences

**Recommendation 72–1** Sections 280(1)(b) and 297 of the *Telecommunications Act 1997* (Cth) should be amended to clarify that the exception does not authorise a use or disclosure that would be permitted by the *Privacy Act* if that use or disclosure would not be otherwise permitted under Part 13 of the *Telecommunications Act*.

**Recommendation 72–2** The *Telecommunications Act 1997* (Cth) should be amended to provide that a use or disclosure of information or a document is permitted if a person has reason to suspect that unlawful activity has been, is being, or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant persons or authorities.

**Recommendation 72–3** The *Telecommunications Act 1997* (Cth) should be amended to provide that a telecommunications service provider may use or disclose 'personal information' as defined in the *Privacy Act* about an individual who is an existing customer aged 15 or over for the purpose of direct marketing only where the:

(a) individual would reasonably expect the organisation to use or disclose the information for the purpose of direct marketing;

(b) organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications; and

(c) the information does not relate to the contents of a communication carried, or being carried, by a telecommunications service provider; or carriage services supplied or intended to be supplied by a telecommunications service provider.

**Recommendation 72–4** The *Telecommunications Act 1997* (Cth) should be amended to provide that a telecommunications service provider may use or disclose 'personal information' as defined in the *Privacy Act* about an individual who is an existing customer and is under 15 years of age for the purpose of direct marketing only in the following circumstances:

(a) either the:

(i) individual has consented; or

(ii) information is not sensitive information and it is impracticable for the organisation to seek the individual's consent before that particular use or disclosure; and

(b) the information does not relate to the contents of a communication carried, or being carried, by a telecommunications service provider; or carriage services supplied or intended to be supplied by a telecommunications service provider;

(c) in each direct marketing communication, the organisation draws to the individual's attention, or prominently displays a notice advising the individual, that he or she may express a wish not to receive any further direct marketing communications;

(d) the organisation provides a simple and functional means by which the individual may advise the organisation that he or she does not wish to receive any further direct marketing communications; and

(e) if requested by the individual, the organisation must, where reasonable and practicable, advise the individual of the source from which it acquired the individual's personal information.

**Recommendation 72–5** The *Telecommunications Act 1997* (Cth) should be amended to provide that in the event that an individual makes a request of an organisation not to receive any further direct marketing communications, the organisation must:

(a) comply with this requirement within a reasonable period of time; and

(b) not charge the individual for giving effect to the request.

**Recommendation 72–6** A note should be inserted after s 280 of the *Telecommunications Act 1997* (Cth) cross-referencing to Chapter 4 (Access to telecommunications data) of the *Telecommunications (Interception and Access) Act 1979* (Cth).

**Recommendation 72–7** Sections 287 and 300 of the *Telecommunications Act 1997* (Cth) should be amended to provide that a use or disclosure by a 'person', as defined under the Act, of information or a document is permitted if:

(a) the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and

(b) the person reasonably believes that the use or disclosure is necessary to lessen or prevent a serious threat to a person's life, health or safety.

**Recommendation 72–8** Section 289 of the *Telecommunications Act 1997* (Cth) should be amended to provide that a use or disclosure by a 'person', as defined under the Act, of information or a document is permitted if the information or document relates to the affairs or personal particulars (including any unlisted telephone number or any address) of another person; and

(a) the other person has consented to the use or disclosure; or

(b) the use or disclosure is made for the purpose for which the information or document came to the person's knowledge or into the person's possession (the primary purpose); or

(c) the use or disclosure is for a purpose other than the primary purpose (the secondary purpose); and

    (i) the secondary purpose is related to the primary purpose, and if the information or document is sensitive information (within the meaning of the *Privacy Act*), the secondary purpose is directly related to the primary purpose; and

    (ii) the other person would reasonably expect the person to use or disclose the information.

**Recommendation 72–9** Part 13 of the *Telecommunications Act 1997* (Cth) should be amended to provide that 'consent' means 'express or implied consent'.

**Recommendation 72–10** Part 13 of the *Telecommunications Act 1997* (Cth) should be amended to provide that use or disclosure by a person of credit reporting information is to be handled in accordance with the *Privacy Act.*

**Recommendation 72–11** The *Telecommunications Act 1997* (Cth) should be amended to clarify when a use or disclosure of information or a document held on the integrated public number database is permitted.

**Recommendation 72–12** Clause 3 of the *Carrier Licence Conditions (Telstra Corporation Limited) Declaration 1997* (Cth) should be amended to provide that 'enforcement agency' has the same meaning as that provided for in the *Telecommunications (Interception and Access) Act 1979* (Cth).

**Recommendation 72–13** Section 285 of the *Telecommunications Act 1997* (Cth) should be amended to provide that a disclosure of an unlisted number is permitted if the disclosure is made to another person for purposes connected with dealing with the matter or matters raised by a call to an emergency service number.

**Recommendation 72–14** The Australian Government should amend s 285(3) of the *Telecommunications Act 1997* (Cth) to provide that before the Minister specifies a kind of research for the purpose of the use or disclosure of information or a document contained in the Integrated Public Number Database, the Minister must be satisfied that the public interest in the relevant research outweighs the public interest in maintaining the level of protection provided by the *Telecommunications Act* to the information in the Integrated Public Number Database.

**Recommendation 72–15** The *Telecommunications (Integrated Public Number Database Scheme—Conditions for Authorisations) Determination 2007 (No 1)* should be amended to provide that an authorisation under the integrated public number database scheme is subject to a condition requiring the holder of the authorisation to notify the Privacy Commissioner, as soon as practicable after becoming aware:

(a) of a substantive or systemic breach of security that reasonably could be regarded as having an adverse impact on the integrity and confidentiality of protected information; and

(b) that a person to whom the holder has disclosed protected information has contravened any legal restrictions governing the person's ability to use or disclose protected information.

**Recommendation 72–16** The *Telecommunications Act 1997* (Cth) should be amended to provide that directory products that are produced from data sources other than the Integrated Public Number Database should be subject to the same rules under Part 13 of the *Telecommunications Act* as directory products which are produced from data sourced from the Integrated Public Number Database.

**Recommendation 72–17** The *Telecommunications Act 1997* (Cth) should be amended to prohibit the charging of a fee for an unlisted (silent) number on a public number directory.

## 73. Other Telecommunications Privacy Issues

**Recommendation 73–1** Section 79 of the *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to provide that the chief officer of an agency must cause a record, including any copy of a record, in the possession of an agency, made by means of an interception to be destroyed when it is no longer needed for a permitted purpose.

**Recommendation 73–2** Section 79 of the *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to require the destruction of non-material content intercepted under a B-Party warrant.

**Recommendation 73–3** The *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to provide that the Australian Security Intelligence Organisation and enforcement agencies must destroy in a timely manner irrelevant material containing accessed telecommunications data which is no longer needed for a permitted purpose.

**Recommendation 73–4** Sections 151 and 163 of the *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to provide for reporting requirements relating to the use of stored communication warrants that are equivalent to the interception warrant reporting requirements under Part 2–7 and s 102 of the Act.

**Recommendation 73–5** The Australian Government Attorney-General's Department should develop and, where appropriate, publish guidance on the interception and access of information under the *Telecommunications (Interception and Access) Act 1979* (Cth), that addresses:

(a) the definition of the term 'telecommunications data';

(b) when voluntary disclosure of telecommunications data to the Australian Security Intelligence Organisation and other enforcement agencies is permitted; and

(c) timeframes within which agencies should review holdings of information and destroy information.

**Recommendation 73–6** The *Telecommunications (Interception and Access) Act 1979* (Cth) should be amended to provide expressly that where the Ombudsman has reason to believe that an officer of an agency is able to give information relevant to an inspection of the agency's records relating to access to a stored communication, the Ombudsman may:

(a) require the officer to give the information to the Ombudsman and to attend a specified place in order to answer questions relevant to the inspection; and

(b) where the Ombudsman does not know the officer's identity, require the chief officer, or a person nominated by the chief officer, to answer questions relevant to the inspection.

**Recommendation 73–7** The Australian Communications and Media Authority should add the Office of the Privacy Commissioner as a member of the Law Enforcement Advisory Committee.

**Recommendation 73–8** The Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman and the Australian Communications and Media Authority should develop memorandums of understanding, addressing:

(a) the roles and functions of each of the bodies under the *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth), *Do Not Call Register Act 2006* (Cth) and *Privacy Act*;

(b) the exchange of relevant information and expertise between the bodies; and

(c) when a matter should be referred to, or received from, the bodies.

**Recommendation 73–9** The document setting out the Office of the Privacy Commissioner's complaint-handling policies and procedures (see Recommendation 49–8), and its enforcement guidelines (see Recommendation 50–3) should address:

(a) the roles and functions of the Office of the Privacy Commissioner, Telecommunications Industry Ombudsman and the Australian Communications and Media Authority under the *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth), *Do Not Call Register Act 2006* (Cth) and *Privacy Act*; and

(b) when a matter will be referred to, or received from, the Telecommunications Industry Ombudsman and the Australian Communications and Media Authority.

**Recommendation 73–10** The Australian Communications and Media Authority, in consultation with relevant stakeholders, should develop and publish guidance relating to privacy in the telecommunications industry. The guidance should:

(a) outline the interaction between the *Privacy Act*, *Telecommunications Act 1997* (Cth), *Spam Act 2003* (Cth) and *Do Not Call Register Act 2006* (Cth);

(b) provide advice on the exceptions under Part 13 of the *Telecommunications Act*, *Spam Act* and the *Do Not Call Register Act*; and

(c) outline what is required to obtain an individual's consent for the purposes of the *Privacy Act*, *Telecommunications Act*, *Spam Act* and *Do Not Call Register Act*. This guidance should cover consent as it applies in various contexts, and include advice on when it is, and is not, appropriate to use the mechanism of 'bundled consent'.

**Recommendation 73–11** The Australian Communications and Media Authority, in consultation with relevant stakeholders, should develop and publish educational material that addresses the:

(a) rules regulating privacy in the telecommunications industry; and

(b) various bodies that are able to deal with a telecommunications privacy complaint, and how to make a complaint to those bodies.

# Part K—Protection of a Right to Personal Privacy

## 74. Protecting a Right to Personal Privacy

**Recommendation 74–1** Federal legislation should provide for a statutory cause of action for a serious invasion of privacy. The Act should contain a non-exhaustive list of the types of invasion that fall within the cause of action. For example, a serious invasion of privacy may occur where:

(a) there has been an interference with an individual's home or family life;

(b) an individual has been subjected to unauthorised surveillance;

(c) an individual's correspondence or private written, oral or electronic communication has been interfered with, misused or disclosed; or

(d) sensitive facts relating to an individual's private life have been disclosed.

**Recommendation 74–2** Federal legislation should provide that, for the purpose of establishing liability under the statutory cause of action for invasion of privacy, a claimant must show that in the circumstances:

(a) there is a reasonable expectation of privacy; and

(b) the act or conduct complained of is highly offensive to a reasonable person of ordinary sensibilities.

In determining whether an individual's privacy has been invaded for the purpose of establishing the cause of action, the court must take into account whether the public interest in maintaining the claimant's privacy outweighs other matters of public interest (including the interest of the public to be informed about matters of public concern and the public interest in allowing freedom of expression).

**Recommendation 74–3** Federal legislation should provide that an action for a serious invasion of privacy:

(a) may only be brought by natural persons;

(b) is actionable without proof of damage; and

(c) is restricted to intentional or reckless acts on the part of the respondent.

**Recommendation 74–4** The range of defences to the statutory cause of action for a serious invasion of privacy provided for in federal legislation should be listed exhaustively. The defences should include that the:

(a) act or conduct was incidental to the exercise of a lawful right of defence of person or property;

(b) act or conduct was required or authorised by or under law; or

(c) publication of the information was, under the law of defamation, privileged.

**Recommendation 74–5** To address a serious invasion of privacy, the court should be empowered to choose the remedy that is most appropriate in the circumstances, free from the jurisdictional constraints that may apply to that remedy in the general law. For example, the court should be empowered to grant any one or more of the following:

(a) damages, including aggravated damages, but not exemplary damages;

(b) an account of profits;

(c) an injunction;

(d) an order requiring the respondent to apologise to the claimant;

(e) a correction order;

(f) an order for the delivery up and destruction of material; and

(g) a declaration.

**Recommendation 74–6** Federal legislation should provide that any action at common law for invasion of a person's privacy should be abolished on enactment of these provisions.

**Recommendation 74–7** The Office of the Privacy Commissioner should provide information to the public concerning the recommended statutory cause of action for a serious invasion of privacy.