Australian Government
Office of the Privacy Commissioner

Approval of the Biometrics Institute Privacy Code

Section 18BB(2) of the *Privacy Act 1988* (Cth)

I, Karen Curtis, Privacy Commissioner, pursuant to section 18BB(2) of the *Privacy Act 1988,* approve the Biometrics Institute Privacy Code which is Schedule 1 of this instrument.

This approval shall take effect on and from **1 September 2006**.

Dated: [19 July 2006]

[signed: Karen Curtis]

Karen Curtis

Privacy Commissioner

Schedule 1

Biometrics Institute

Privacy Code

19 July 2006

Biometrics Institute Ltd
PO Box 576, Crows Nest NSW 1585, Australia
Ph: +61 2 9431 8686
Fax: +61 2 9431 8677
Email: manager@biometricsinstitute.org
www.biometricsinstitute.org

BIOMETRICS INSTITUTE PRIVACY CODE

A. PREAMBLE

1. The Biometrics Institute is an independent, not-for-profit organisation founded in 2001 with the purpose of promoting the responsible use and development of biometric technologies. The Biometrics Institute has decided to develop a Biometrics Institute Privacy Code, as provided for under the *Privacy Act 1988 1988 (Commonwealth).*

2. The Biometrics Institute Privacy Code seeks to build upon the National Privacy Principles (NPPs) in a manner that provides the community with the assurance needed to encourage informed and voluntary participation in biometrics programs. Biometrics Institute members understand that only by adopting and promoting ethical practices, openness and transparency can these technologies gain widespread acceptance.

3. The obligations in the Biometrics Institute Privacy Principles contained in this Biometrics Institute Privacy Code are substantially the same to those set out in Schedule 3 to the Privacy Act. Where the Supplementary Biometrics Institute Privacy Principles have been introduced into the Biometrics Institute Privacy Code, they are intended to provide additional privacy protection to end-users, not to alter the meaning or effect of the NPPs.

4. The Code is expected not only to fulfil its functions under the Privacy Act but also to positively promote the importance of individuals' privacy across the biometrics and related industries and to help educate consumers in their privacy rights.

5. The Office of the Privacy Commissioner approved the Code on 19 July 2006. This approval indicates that the Commissioner is satisfied that the Biometrics Institute Privacy Principles included in this Code are at least the overall equivalent of all of the obligations set out in the National Privacy Principles in the Privacy Act.

6. Administration of the Code is the responsibility of the Biometrics Institute Secretariat, under direction of its Board and is subject to independent review by the Independent Code Review Panel and the Office of the Privacy Commissioner.

Federal Register of Legislative Instruments F2006L02406

B. OBJECTIVES

1. The aims of this Code are

   1.1 to facilitate the protection of personal information provided by, or held in relation to, biometric systems;

   1.2 to facilitate the process of identity authentication in a manner consistent with the Privacy Act and the NPPs; and

   1.3 to promote biometrics as privacy enhancing technologies (PETs).

C. APPLICATION

1. This Code is binding upon organisations that have agreed to be covered by the Code by signing the 'Biometrics Institute Privacy Code Agreement to Comply'.

2. Only members of the Biometrics Institute are eligible to subscribe to this Code.

3. Biometrics Institute membership, and thus subscription to this Code, is voluntary.

4. Government agencies at both a state and federal level may choose to follow the Code; they may also prefer tenderers to be signatories to the Code. However, Australian Government agencies are not legally required to comply with the Code.

5. The Biometrics Institute will maintain an up to date and publicly available register of Code Subscribers bound by this Code.

6. The Board may review the criteria for eligibility from time to time.

D. COVERAGE

Exempt acts and practices

1. Some categories of acts and practices are exempt from the regulation of the National Privacy Principles (per sections 7B, 7C of the Privacy Act).
2. Privacy Codes made under the Privacy Act, however, may cover these otherwise exempt acts and practices (this is permitted by section 18BAA).
3. In accordance with subsections 7B(1), (2), (4), (5) and section 7C, acts and practices by individuals acting in a non-business capacity, organisations acting under Commonwealth contract, organisations acting in the course of journalism, organisations acting under a State or Territory contract, and political acts and practices, remain exempt under this Code.

Federal Register of Legislative Instruments F2006L02406

Employee records

4. Acts or practices of employer organisations which are directly related to a current or former employment relationship between the employer and an individual, and are also directly related to an employee record held by the organisation relating to that individual, are exempt from the National Privacy Principles (see section 7B(3)).
5. However, as permitted by section 18BAA, this Code covers the acts and practices described in clause D.4 where a biometric is included as part of the employee record, or where a biometric has a function related to the collection and storage of, access to or transmission of that employee record.
6. The aim of clause D.5 is to ensure that this Code regulates the handling of employee records in which a biometric is stored, as well as those employee records which are protected by a biometric. The handling of such records may otherwise be exempt under the Privacy Act.
7. The handling of employee records which do not involve a biometric in the manner described in clause D.5 remains exempt from this Code in accordance with section 7B(3).
8. Nothing in clauses D.4-7 should be read as causing acts and practices referred to in clause D.3 to be covered by this Code.

Note: Despite the exemption in the Privacy Act, a Code may cover exempt Acts and Practices.

E. INTERPRETATION

Nothing in the Supplementary Biometrics Institute Privacy Principles (Principles 11, 12, 13) removes or reduces an obligation in the Biometrics Institute Privacy Principles (Principles 1 to 10).

Other than as defined below, words used in this Code have the meaning defined in the Privacy Act as amended from time to time.

Approved privacy code means

(a) a privacy code approved by the Commissioner under section 18BB of the Privacy Act; or
(b) a privacy code approved by the Commissioner under section 18BB of the Privacy Act with variations approved by the Commissioner under section 18BD.

Biometric means the biological or behavioural unique characteristic of an individual which is captured for the purposes of identification and/ or verification of the individual.

Biometric Information is any data that can be used to biometrically identify an individual. This data includes, but is not limited to, images, sounds, chemical or geometric properties. It also includes any information encrypted or unencrypted that is derived from these raw acquired biometrics, such as biometric templates or filtered or pre-processed data. It does not include non-biometric

information such as name and address. It also does not include simple single factor biometric measurements, such as age, height, eye colour and place of birth, unless such simple single factor biometric measurements are used for automated verification purposes.

Biometric Providers means an individual or an organisation that provides a service and/ or product related to the installation, management of or integration of biometrics.

Biometric System means a system which uses biometrics to identify and/ or verify an individual.

Biometrics means automated methods for identifying and/or verifying an individual on the basis of some biological or behavioural unique characteristic of the individual.

Biometrics Institute Privacy Code Agreement to Comply means the agreement signed by a Code Subscriber to comply with the Biometrics Institute Privacy Code.

Code means this Biometrics Institute Privacy Code.

Code Administrator means the body outlined in subclause H.1.

Code Subscriber means an organisation that has agreed to be bound by the Code and has been approved by the Board of the Biometrics Institute in accordance with clause K.

Collection includes gathering, acquiring or obtaining information from any source, by any means. Collection may be directly from an individual or indirectly from another person or organisation. In practical terms, for biometrics, collection is likely to include, but not be limited to, the enrolment of an individual in a biometric system.

Commonwealth contract means a contract, to which the Commonwealth or an agency (as defined in the Privacy Act) is or was a party, under which services are to be, or were to be, provided to an agency.

Consent means free and informed agreement with what is being done or proposed. Consent can be either express or implied. Express consent is given explicitly, either orally or in writing. Express consent is unequivocal and does not require any inference on the part of the organisation seeking consent. Implied consent arises where consent may reasonably be inferred from the action or inaction of the individual.

Contact details means a record of personal information such as names, companies, position titles, addresses and phone numbers, collected and retained in order to contact individuals.

Contracted service provider, for a government contract, means:

(a) an organisation that is or was a party to the government contract and that is or was responsible for the provision of services to a government agency under the government contract; or

(b) a subcontractor for the government contract.

Correct, in relation to personal information, means to alter that information by way of amendment, enhancement, deletion or addition.

De-identification means the removal of personal information or any details that identify the individual, or from which the identity of the individual can reasonably be ascertained, without retaining a means by which the information could be easily re-identified.

Disclose in relation to personal information, includes making personal information available to others outside the organisation, other than the subject of the information. Disclosure includes the publication of personal information through any medium.

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

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

Encryption means encoding data such that a third party, including one with knowledge of the algorithm, cannot read or use the biometric without the use of a cryptographic key.

Enforcement body means:

(a) the Australian Federal Police; or
(b) the Australian Crime Commission; or
(c) the Australian Customs Service; or
(d) the Australian Prudential Regulation Authority; or
(e) the Australian Securities and Investments Commission; or
(f) another agency, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law; or
(g) another agency, to the extent that it is responsible for administering a law relating to the protection of the public revenue; or
(h) a police force or service of a State or a Territory; or
(i) the New South Wales Crime Commission; or
(j) the Independent Commission Against Corruption of New South Wales; or
(k) the Police Integrity Commission of New South Wales; or

(l) the Criminal Justice Commission of Queensland; or
(m) another prescribed authority or body that is established under a law of a State or Territory to conduct criminal investigations or inquiries; or
(n) a State or Territory authority, to the extent that it is responsible for administering, or performing a function under, a law that imposes a penalty or sanction or a prescribed law; or
(o) a State or Territory authority, to the extent that it is responsible for administering a law relating to the protection of the public revenue.

Function creep, when used in connection with Biometrics, means the risk that a biometric collected for one stated purpose being subsequently used or disclosed for another purpose without the knowledge and/or consent to the individual involved.

Government contract means a Commonwealth contract or a State contract.

Health service means:
(a) an activity performed in relation to an individual that is intended or claimed (expressly or otherwise) by the individual or the person performing it:
    (i) to assess, record, maintain or improve the individual's health; or
    (ii) to diagnose the individual's illness or disability; or
    (iii) to treat the individual's illness or disability or suspected illness or disability; or
(b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

Individual means a natural person.

Independent Code Review Panel means the body established under subclause I.1.

Interference with privacy, in relation to an individual, has the meaning given in section 13A of the Privacy Act and includes an act or practice of an organisation that breaches an approved privacy code that binds the organisation in relation to personal information that relates to the individual.

Internal privacy complaint procedure, in relation to a Biometrics Institute Privacy Code Subscriber, means the Code Subscriber's internal procedure for handling a privacy complaint, as distinct from the procedures that are external to an organisation for handling a privacy complaint and that involve the Office of the Privacy Commissioner (as provided for by the Biometrics Institute Privacy Code).

National Privacy Principles mean the National Privacy Principles contained in Schedule 3 of the Privacy Act. A reference to a National Privacy Principle by number is a reference to the clause of Schedule 3 with that number.

Organisation means:
(a) an individual; or
(b) a body corporate; or
(c) a partnership; or
(d) any other unincorporated association; or
(e) a trust;

that is not a small business operator, a registered political party, an 'agency' (as defined by the Privacy Act), a State or Territory authority or a prescribed instrumentality of a State or Territory (as defined by the Privacy Act).
(See section 6C of the Privacy Act for additional information on this definition.)

Person includes an organisation.

Personal information means information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion.
Privacy Act means the *Privacy Act 1988 (Commonwealth)* as amended.
Privacy complaint means a complaint about an alleged interference with the privacy of an individual by an organisation that is subject to the Biometrics Institute Privacy Code.

Public Register means the register of Code Subscribers maintained by the Code Administrator in accordance with subclause H.3.2.

Reasonable steps mean such steps (if any) as are, in the circumstances, reasonable.

Small business has the meaning given in section 6D of the Privacy Act.

Small business operator has the meaning given in section 6D of the Privacy Act.

State or Territory authority has the meaning given by section 6C of the Privacy Act.

Transfer includes the physical or electronic release of information outside an organisation. This includes when a Code Subscriber gives another organisation information under contract to carry out an activity.

Unreasonably intrusive includes any collection of information where the subject or manner is likely to cause unreasonable inconvenience, or to upset or offend an individual.

Federal Register of Legislative Instruments F2006L02406

F. BIOMETRICS INSTITUTE PRIVACY PRINCIPLES

1 Collection

1.1 A Code Subscriber must not collect personal information unless the information is necessary for one or more of its functions or activities.

1.2 A Code Subscriber must collect personal information only by lawful and fair means and not in an unreasonably intrusive way.

1.3 At or before the time (or as soon as practicable after) a Code Subscriber collects personal information from the individual, the Code Subscriber must take reasonable steps to ensure that the individual is aware of

(a) the identity of the Code Subscriber and how to contact it; and

(b) the fact that he or she is able to gain access to the information; and

(c) the purposes for which the information is collected; and

(d) the organisations (or the types of organisations) to which the Code Subscriber usually discloses information of that kind; and

(e) any law that requires the particular information to be collected; and

(f) the main consequences (if any) for the individual if all or part of the information is not provided.

1.4 If it is reasonable and practicable to do so, a Code Subscriber must collect personal information about an individual only from that individual.

1.5 If a Code Subscriber collects personal information about an individual from someone else, it must take reasonable steps to ensure that the individual is or has been made aware of the matters listed in clause 1.3 except to the extent that making the individual aware of those matters would pose a serious threat to the life or health of any individual.

Note: Biometrics Institute Privacy Principle 10 sets out additional rules for the collection of sensitive personal information.

2 Use and disclosure

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

(a) both of the following apply:

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

(ii) the individual would reasonably expect the Code Subscriber to use or disclose the information for the secondary purpose; or

(b) the individual has consented to the use or disclosure; or

(c) if the information is not sensitive information and the use of the information is for the secondary purpose of direct marketing:

(i) it is impracticable for the Code Subscriber to seek the individual's consent before that particular use; and

(ii) the Code Subscriber will not charge the individual for giving effect to a request by the individual to the Code Subscriber not to receive direct marketing communications; and

(iii) the individual has not made a request to the Code Subscriber not to receive direct marketing communications; and

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

(v) each written direct marketing communication by the Code Subscriber with the individual (up to and including the communication that involves the use) sets out the Code Subscriber's business address and telephone number and, if the communication with the individual is made by fax, telex or other electronic means, a number or address at which the Code Subscriber can be directly contacted electronically; or

(d) if the information is health information and the use or disclosure is necessary for research, or the compilation or analysis of statistics, relevant to public health or public safety:

(i) it is impracticable for the Code Subscriber to seek the individual's consent before the use or disclosure; and

(ii) the use or disclosure is conducted in accordance with guidelines approved by the Commissioner under s. 95A of the Privacy Act; and

(iii) in the case of disclosure—the Code Subscriber reasonably believes that the recipient of the health information will not disclose the health information, or personal information derived from the health information; or

(e) the Code Subscriber reasonably believes that the use or disclosure is necessary to lessen or prevent:

(i) a serious and imminent threat to an individual's life, health or safety; or

(ii) a serious threat to public health or public safety; or

(f) the Code Subscriber 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; or

(g) the use or disclosure is required or authorised by or under law; or

(h) the Code Subscriber reasonably believes that the use or disclosure is reasonably necessary for one or more of the following by or on behalf of an enforcement body:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law;

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime;

(iii) the protection of the public revenue;

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct;

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of the orders of a court or tribunal.

Note 1: It is not intended to deter Code Subscribers from lawfully co-operating with agencies performing law enforcement functions in the performance of their functions.

Note 2: Subclause 2.1 does not override any existing legal obligations not to disclose personal information. Nothing in subclause 2.1 requires a Code Subscriber to disclose personal information; a Code Subscriber is always entitled not to disclose personal information in the absence of a legal obligation to disclose it.

Note 3: A Code Subscriber is also subject to the requirements of Biometrics Institute Privacy Principle 9 if it transfers personal information to a person in a foreign country.

2.2 If a Code Subscriber uses or discloses personal information under paragraph 2.1(h), it must make a written note of the use or disclosure.

2.3 Subclause 2.1 operates in relation to personal information that a Code Subscriber that is a body corporate has collected from a related body corporate as if the Code Subscriber's primary purpose of collection of the information were the primary purpose for which the related body corporate collected the information.

2.4 Despite subclause 2.1, a Code Subscriber 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:

(a) the individual:

(i) is physically or legally incapable of giving consent to the disclosure; or

(ii) physically cannot communicate consent to the disclosure; and

(b) a natural person (the ***carer***) providing the health service for the Code Subscriber is satisfied that either:

(i) the disclosure is necessary to provide appropriate care or treatment of the individual; or

(ii) the disclosure is made for compassionate reasons; and

(c) the disclosure is not contrary to any wish:

(i) expressed by the individual before the individual became unable to give or communicate consent; and

(ii) of which the carer is aware, or of which the carer could reasonably be expected to be aware; and

(d) the disclosure is limited to the extent reasonable and necessary for a purpose mentioned in paragraph (b).

2.5 For the purposes of subclause 2.4, a person is ***responsible*** for an individual if the person is:

(a) a parent of the individual; or

(b) a child or sibling of the individual and at least 18 years old; or

(c) a spouse or de facto spouse of the individual; or

(d) a relative of the individual, at least 18 years old and a member of the individual's household; or

(e) a guardian of the individual; or

(f) exercising an enduring power of attorney granted by the individual that is exercisable in relation to decisions about the individual's health; or

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

(h) a person nominated by the individual to be contacted in case of emergency.

2.6 In subclause 2.5:

child of an individual includes an adopted child, a step-child and a foster-child, of the individual.

parent of an individual includes a step-parent, adoptive parent and a foster-parent, of the individual.

relative of an individual means a grandparent, grandchild, uncle, aunt, nephew or niece, of the individual.

sibling of an individual includes a half-brother, half-sister, adoptive brother, adoptive sister, step-brother, step-sister, foster-brother and foster-sister, of the individual.

3 Data quality

A Code Subscriber must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and up-to-date.

4 Data security

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

4.2 A Code Subscriber must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under Biometrics Institute Privacy Principle 2.

5 Openness

5.1 A Code Subscriber must set out in a document clearly expressed policies on its management of personal information. The Code Subscriber must make the document available to anyone who asks for it.

5.2 On request by a person, a Code Subscriber must take reasonable steps to let the person know, generally, what sort of personal information it holds,

for what purposes, and how it collects, holds, uses and discloses that information.

6 Access and correction

6.1 If a Code Subscriber holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

(a) in the case of personal information other than health information—providing access would pose a serious and imminent threat to the life or health of any individual; or

(b) in the case of health information—providing access would pose a serious threat to the life or health of any individual; or

(c) providing access would have an unreasonable impact upon the privacy of other individuals; or

(d) the request for access is frivolous or vexatious; or

(e) the information relates to existing or anticipated legal proceedings between the Code Subscriber and the individual, and the information would not be accessible by the process of discovery in those proceedings; or

(f) providing access would reveal the intentions of the Code Subscriber in relation to negotiations with the individual in such a way as to prejudice those negotiations; or

(g) providing access would be unlawful; or

(h) denying access is required or authorised by or under law; or

(i) providing access would be likely to prejudice an investigation of possible unlawful activity; or

(j) providing access would be likely to prejudice:

(i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or

(ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of the public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;

by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks the Code Subscriber not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

6.2 However, where providing access would reveal evaluative information generated within the Code Subscriber in connection with a commercially sensitive decision-making process, the Code Subscriber may give the

individual an explanation for the commercially sensitive decision rather than direct access to the information.

Note: A Code Subscriber breaches subclause 6.1 if it relies on subclause 6.2 to give an individual an explanation for a commercially sensitive decision in circumstances where subclause 6.2 does not apply.

6.3 If the Code Subscriber is not required to provide the individual with access to the information because of one or more of paragraphs 6.1(a) to (k) (inclusive), the Code Subscriber must, if reasonable, consider whether the use of mutually agreed intermediaries would allow sufficient access to meet the needs of both parties.

6.4 If a Code Subscriber charges for providing access to personal information, those charges:

(a) must not be excessive; and

(b) must not apply to lodging a request for access.

6.5 If a Code Subscriber holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the Code Subscriber must take reasonable steps to correct the information so that it is accurate, complete and up-to-date.

6.6 If the individual and the Code Subscriber disagree about whether the information is accurate, complete and up-to-date, and the individual asks the Code Subscriber to associate with the information a statement claiming that the information is not accurate, complete or up-to-date, the Code Subscriber must take reasonable steps to do so.

6.7 A Code Subscriber must provide reasons for denial of access or a refusal to correct personal information.

7 Identifiers

7.1 A Code Subscriber must not adopt as its own identifier of an individual an identifier of the individual that has been assigned by:

(a) an agency; or

(b) an agent of an agency acting in its capacity as agent; or

(c) a contracted service provider for a Commonwealth contract acting in its capacity as contracted service provider for that contract.

7.1A However, subclause 7.1 does not apply to the adoption by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before those matters are prescribed: see subsection 100(2) of the Privacy Act.

7.2 A Code Subscriber must not use or disclose an identifier assigned to an individual by an agency, or by an agent or contracted service provider mentioned in subclause 7.1, unless:

(a) the use or disclosure is necessary for the Code Subscriber to fulfil its obligations to the agency; or

(b) one or more of paragraphs 2.1(e) to 2.1(h) (inclusive) apply to the use or disclosure; or

(c) the use or disclosure is by a prescribed organisation of a prescribed identifier in prescribed circumstances.

Note: There are prerequisites that must be satisfied before the matters mentioned in paragraph (c) are prescribed: see subsection 100(2) and (3) of the Privacy Act.

7.3 In this clause:

identifier includes a number assigned by a Code Subscriber to an individual to identify uniquely the individual for the purposes of the Code Subscriber's operations. However, an individual's name or ABN (as defined in the *A New Tax System (Australian Business Number) Act 1999*) is not an ***identifier***.

8 Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with a Code Subscriber.

9 Transborder data flows

A Code Subscriber in Australia or an external Territory may transfer personal information about an individual to someone (other than the Code Subscriber or the individual) who is in a foreign country only if:

(a) the Code Subscriber reasonably believes that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are substantially similar to the National Privacy Principles; or

(b) the individual consents to the transfer; or

(c) the transfer is necessary for the performance of a contract between the individual and the Code Subscriber, or for the implementation of pre-contractual measures taken in response to the individual's request; or

(d) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the individual between the Code Subscriber and a third party; or

(e) all of the following apply:

(i) the transfer is for the benefit of the individual;

(ii) it is impracticable to obtain the consent of the individual to that transfer;

(iii) if it were practicable to obtain such consent, the individual would be likely to give it; or

(f) the Code Subscriber has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the Biometrics Institute Privacy Principles.

10 Sensitive information

10.1 A Code Subscriber must not collect sensitive information about an individual unless:

(a) the individual has consented; or

(b) the collection is required by law; or

(c) the collection is necessary to prevent or lessen a serious and imminent threat to the life or health of any individual, where the individual whom the information concerns:

(i) is physically or legally incapable of giving consent to the collection; or

(ii) physically cannot communicate consent to the collection; or

(d) if the information is collected in the course of the activities of a non-profit Code Subscriber—the following conditions are satisfied:

(i) the information relates solely to the members of the Code Subscriber or to individuals who have regular contact with it in connection with its activities;

(ii) at or before the time of collecting the information, the Code Subscriber undertakes to the individual whom the information concerns that the Code Subscriber will not disclose the information without the individual's consent; or

(e) the collection is necessary for the establishment, exercise or defence of a legal or equitable claim.

10.2 Despite subclause 10.1, a Code Subscriber may collect health information about an individual if:

(a) the information is necessary to provide a health service to the individual; and

(b) the information is collected:

(i) as required by law (other than the Privacy Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the Code Subscriber.

10.3 Despite subclause 10.1, a Code Subscriber may collect health information about an individual if:

(a) the collection is necessary for any of the following purposes:

(i) research relevant to public health or public safety;

(ii) the compilation or analysis of statistics relevant to public health or public safety;

(iii) the management, funding or monitoring of a health service; and

(b) that purpose cannot be served by the collection of information that does not identify the individual or from which the individual's identity cannot reasonably be ascertained; and

(c) it is impracticable for the Code Subscriber to seek the individual's consent to the collection; and

(d) the information is collected:

(i) as required by law (other than the Privacy Act); or

(ii) in accordance with rules established by competent health or medical bodies that deal with obligations of professional confidentiality which bind the Code Subscriber; or

(iii) in accordance with guidelines approved by the Commissioner under s. 95A of the Privacy Act.

10.4 If a Code Subscriber collects health information about an individual in accordance with subclause 10.3, the Code Subscriber must take reasonable steps to permanently de-identify the information before the Code Subscriber discloses it.

10.5 In this clause:

non-profit Code Subscriber means a non-profit Code Subscriber that has only racial, ethnic, political, religious, philosophical, professional, trade, or trade union aims.

SUPPLEMENTARY BIOMETRICS INSTITUTE PRIVACY PRINCIPLES

11 Protection

11.1 Wherever practicable, a Code Subscriber shall ensure that biometric information is encrypted immediately after collection, that the original biometric information is destroyed after encryption and that biometric information is stored only in encrypted form.

11.2 Biometric information shall be held separately from other personal information the Code Subscriber may hold. Where practicable, biometric information shall be de-identified such as through removal of the name from any proximity to the biometric information. That biometric information shall be held in such a way that it cannot easily be matched with personal information.

11.3 Unless required by law, biometric information shall remain in storage only as long as is necessary for the proper functioning of the biometric system for which it was collected.

11.4 After personal information is no longer needed for any purpose for which it may be used or disclosed under Biometrics Institute Privacy Principle 2, it shall be destroyed or otherwise disposed of in a secure manner as outlined in Biometrics Institute Privacy Principle 4.2.

11.5 Transmissions of a biometric shall be undertaken with due care, giving due regard to the security of the medium involved.

11.6 Access to biometric information shall be limited to those within the Code Subscriber with a specific need to have access in order to fulfill their job functions. Code Subscribers will maintain records showing which individuals within their organisation have access to a biometric.

Note: In relation to clause 11 refer to Biometrics Institute Privacy Principle 4 as it has closely associated obligations

12 Control

12.1 Enrolments in biometric systems shall be voluntary, unless required by law.

12.2 Individuals who have enrolled in a biometric system shall be informed of any change in the scope or purpose of the system.

Note: Refer to Biometrics Institute Privacy Principles 1.3, 1.5, 2 as they have closely associated obligations

12.3 Secondary analysis or function creep of biometric information collected for purposes such as authentication or identification is not permitted without express free and informed consent. For example biometric information collected for the purposes of authentication and identification shall not be used to examine that information in search of genetic patterns or disease identification without express free and informed consent.

Note: Refer to Biometrics Institute Privacy Principle 2 as it has closely associated obligations

12.4 Individuals who have enrolled in a biometric system shall, where possible, and upon request, be given the opportunity to have their biometric information removed from the system.

Note: Refer to Biometrics Institute Privacy Principle 4 as it has closely associated obligations

13 Accountability

13.1 Code Subscribers shall disclose the purpose(s) for which a biometric system is being deployed.

Note: Refer to Biometrics Institute Privacy Principle 1 as it has closely associated obligations

13.2 Auditing of biometric systems by a third party shall be implemented. The audit must examine compliance with all the Biometrics Institute Privacy Principles, in particular

- access controls and procedures for biometric systems and related systems including personnel procedures relating to enrolment, protection of the biometric and its storage and disposal
- privacy policies including distribution and compliance checking
- staff privacy training and awareness procedures
- review and assurance procedures for privacy and biometrics
- technical systems security
- information protection procedures
- complaint procedures

Note: Refer to Biometrics Institute Privacy Principles 4, and 5.1 as they have closely associated obligations

13.3 A Code Subscriber must consider "end-to-end" privacy management issues when providing a product or service to an information technology system. This is a regime which covers at least the secure collection, storage and transmission of biometrics and any associated records. This also includes privacy audits, privacy impact statements, access control and other procedures related to a holistic privacy policy and procedures regime. This requires biometric providers to take a holistic view of their role in managing privacy across an enterprise.

Note: Refer to Biometrics Institute Privacy Principle 4.1 as it has closely associated obligations

13.4 A Code Subscriber shall conduct privacy impact assessments as part of the planning and management process for biometrics implementation.

G. STANDARDS

Code Subscribers must be aware of and take account of the relevant national and international standards for information protection and biometric systems which prevail from time to time. Depending on the jurisdiction and role of Code Subscribers these may include:

- AS/NZS ISO/IEC 17799:2001 Information technology - Code of practice for information security management, produced by Standards Australia
- AS/NZS ISO/IEC 27001:2006 Information technology - Security techniques - Information security management systems - Requirements
- Australian Communications Security Instruction (ACSI) 33 Australian Government Information and Communications Technology Security Manual, produced by the Defence Signals Directorate
- Australian Government's Protective Security Manual (PSM), produced by the Attorney-General's Department
- International Standards produced by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC) and their Australian adoptions, produced by Standards Australia, such as:
    - ISO/IEC 19784-1:2006 Information technology - Biometric application programming interface - Part 1: BioAPI specification
    - ISO/IEC 19785-1:2006 Information technology - Common Biometric Exchange Formats Framework - Part 1: Data element specification
    - ISO/IEC 19785-2:2006 Information technology - Common Biometric Exchange Formats Framework - Part 2: Procedures for the operation of the Biometric Registration Authority
    - ISO/IEC 19794-1:2006 Information technology - Biometric data interchange formats - Part 1: Framework
    - ISO/IEC 19794-2:2005 Information technology - Biometric data interchange formats - Part 2: Finger minutiae data
    - ISO/IEC 19794-4:2005 Information technology - Biometric data interchange formats - Part 4: Finger image data
    - ISO/IEC 19794-5:2005 Information technology - Biometric data interchange formats - Part 5: Face image data

- ISO/IEC 19794-6:2005 Information technology - Biometric data interchange formats - Part 6: Iris image data
- ISO/IEC 19795-1:2006 Information technology - Biometric performance testing and reporting -- Part 1: Principles and framework

- Relevant travel document standards, produced by bodies including the International Civil Aviation Organization.

H. ADMINISTRATION

Code Administrator

1. This Code is administered by the Biometrics Institute Secretariat ('Code Administrator'), under direction of the Biometrics Institute Board, which comprises:
   1.1 the Biometrics Institute Executive Officer; and
   1.2 such other persons as the Biometrics Institute Board may from time to time nominate.

2. The Code Administrator will be funded by Biometrics Institute in such manner, as the Biometrics Institute Board considers appropriate, having regard to the resource requirements necessary for the effective execution of those tasks described in subclause H.3.

Tasks of the Code Administrator

3. In administering this Code, the Code Administrator will perform the following tasks:
   3.1 manage the registration of Code Subscribers; and
   3.2 maintain an accurate and up to date online Public Register of Code Subscribers; and
   3.3 produce a written response to the report produced by the Independent Code Review Panel under subclause I.3, which will be submitted, along with the report, to the Privacy Commissioner within 30 business days of the report's being finalised; and
   3.4 perform such other tasks as the Biometrics Institute Board considers necessary or desirable for the effective operation of the Code.

I. REVIEW

Independent Code Review Panel

1. This Code is subject to independent review by the Independent Code Review Panel, which comprises:
   1.1 an independent chairperson; and
   1.2 an equal number of consumer and industry representatives which the Biometrics Institute Board may from time to time nominate.

2. The Independent Code Review Panel will be funded by Biometrics Institute in such manner as the Biometrics Institute Board considers appropriate, having regard to the resource requirements necessary for the effective execution of its tasks.

Tasks of Independent Code Review Panel

3. The Independent Code Review Panel will:
    3.1 within 3 years after registration of this Code, and once every three years thereafter, produce a report on the operation of the code, which will be submitted, along with the Code Administrator's written response to this report, to the Privacy Commissioner within 30 business days of the report's being finalised; and
    3.2 recommend amendments to the Code, at any time that it considers them necessary or desirable for the effective operation of the Code, on request or by its own initiative; and
    3.3 where an amendment has been recommended complete the steps necessary to make an amendment to the Code referred to in subclause I.6.

4. The steps referred to in subclauses I.3.1 to 3.3 shall together provide a basis for ensuring that the Code is meeting its objectives and remains relevant and up to date.

Consultation

5. In conducting the review under subclause I.3, the Independent Code Review Panel will:
    5.1 direct the Code Administrator to notify the Office of the Privacy Commissioner of the review; and
    5.2 seek the views of the Privacy Commissioner, government agencies, industry representatives, consumer representatives, the general public and other persons or bodies as appropriate in Australia and internationally, regarding the operation of the Code and in relation to suitable revisions and amendments.

Amendment Procedure

6. To amend the Code, the Independent Code Review Panel must complete the following steps:
    6.1 In accordance with section 18BD of the Privacy Act, unless the amendment is likely to be considered a minor variation by the Privacy Commissioner:
        (a) seek the views of the Privacy Commissioner, government agencies, industry representatives, consumer representatives, the general public and other persons or bodies as appropriate in Australia and internationally, regarding the proposed amendment; and
        (b) resolve the terms of any proposed amendment; and
    6.2 give notice of the terms of the proposed amendment to each Code Subscriber and the general public; and
    6.3 allow 60 business days to provide comments to Independent Code Review Panel; and
    6.4 adopt or reject the proposed amendment with or without modifications (not including modifications that would make the proposed amendment substantively different to that originally proposed); and
    6.5 obtain the approval of the Biometrics Institute Board; and
    6.6 seek the approval of the Privacy Commissioner; and

6.7 if the Privacy Commissioner approves the amendment, notice of the amendment must be given to Code Subscribers, Biometrics Institute Members and any other relevant stakeholders as identified by the Biometrics Institute Board.

7. Any application to the Privacy Commissioner for an amendment to the Code should be expressed to take effect not earlier than 30 days after approval.

J. COMPLAINTS

Internal Privacy Complaint Procedures

1. Code Subscribers will ensure that they make available a copy of the Code and any explanatory material on request, and that they have in place publicly available procedures for dealing with a complaint from inception to satisfaction or determination, which are available to any individual (irrespective of nationality or place of residence) about whom personal information is held. Such procedures should be in line with Australian Standard AS4269.

Code Subscribers and Transparency

2. Code Subscribers will deal with all formal complaints promptly and transparently, keeping the complainant informed about progress of their complaint.

Time for Resolution and Referral to Privacy Commissioner

3. If a complaint cannot be resolved to the satisfaction of the complainant within 30 business days, either the complainant or the Code Subscriber with the consent of the complainant may refer the complaint to the Privacy Commissioner.

K. REGISTRATION AND DEREGISTRATION

Application to become a Code Subscriber

1. Organisations eligible to be Code Subscribers may make application to the Code Administrator in accordance with the procedures established by the Code Administrator and approved by the Biometrics Institute Board from time to time.

2. If an applicant intends that its registration as a Code Subscriber is to cover one or more subsidiaries, then, subject to each subsidiary being eligible for registration, the applicant must provide the names of each subsidiary organisation in its application.

3. The application shall be in a form prescribed by the Code Administrator and approved by the Biometrics Institute Board from time to time and will include a duly authorised and signed Biometrics Institute Privacy Code Agreement to Comply by the applicant indicating that it agrees to be bound by the Code.

4. The Code Administrator will, within a reasonable time:
   4.1 assess the eligibility of the applicant for approval as a Code Subscriber; and
   4.2 upon satisfying itself that an applicant is eligible for approval as a Code Subscriber recommend to the Biometrics Institute Board that the relevant application be approved.

5. Where, in the course of assessing an application under subclause K.4, the Code Administrator finds an applicant to be ineligible for approval, the Code Administrator will notify the applicant, setting out the reasons for its ineligibility.

6. An applicant who is notified of their ineligibility under subclause K.5 shall have the opportunity of rectifying their ineligibility and reapplying for approval.

7. The Biometrics Institute Board will periodically consider all recommendations for approval of applications by the Code Administrator and will notify the Code Administrator of its decision to ratify or otherwise reject each application.

8. If the Biometrics Institute Board decides not to ratify the Code Administrator's recommendation under subclause K.4.2, it shall provide the Code Administrator with reasons, whereupon the Code Administrator will notify the applicant of its unsuccessful application, together with reasons.

9. Neither:
   9.1 refusal by the Biometrics Institute Board to ratify an application; nor
   9.2 deregistration in accordance with subclause K.19, will prevent a Code Subscriber or applicant as the case may be from reapplying at a later stage for registration, provided that:
   9.3 such application is made in good faith; and
   9.4 in the case of re-registration, the applicant satisfies the Biometrics Institute Board that:
      (a) it is willing to comply with the Code; and
      (b) it has adequate procedures in place to do so; and
      (c) it has taken all reasonable steps to ensure that it is capable of complying with the Code.

Procedure Upon Approval

10. Upon approval of an application, the Code Administrator will:
   10.1 notify in writing the applicant of the approval; and
   10.2 add the name of the applicant to the Public Register.

11. The steps referred to in subclause K.10 shall constitute registration of a Code Subscriber, and shall take effect from the date that the notification referred to in subclause K.10.1 is sent by the Code Administrator.

Public Information Resource

12. The Code Administrator shall cause to be published on the Biometrics Institute website
www.biometricsinstitute.org an easily accessible public information resource which contains:
   12.1 the Public Register of current Code Subscribers; and
   12.2 information about the Code; and
   12.3 a copy of the most current version of the Code; and
   12.4 contact details for the Code Administrator; and
   12.5 information about making a complaint in relation to matters contained in the Code; and

12.6 a link to the website of the Office of the Privacy Commissioner; and
12.7 any other information that the Code Administrator considers relevant to the efficient functioning of the Code.

Improper conduct

13. If a Code Subscriber acts in a manner that, in the Biometrics Institute Board's discretion,
constitutes seriously improper conduct in relation to the Code, then the Biometrics Institute
Board shall direct the Code Administrator to notify the Code Subscriber of the breach.

14. Within 7 business days of receipt of such notification, the Code Subscriber must:
14.1 take all reasonable steps to rectify the seriously improper conduct; and
14.2 notify the Code Administrator of the steps taken to rectify the seriously improper conduct.

15. If the Code Subscriber fails to adequately comply with subclause K.14, then the Biometrics Institute Board will issue a final notice requiring the Code Subscriber to rectify the seriously improper conduct within seven (7) business days.

16. The provisions in subclauses K.13 to K.15 and K.17.1 shall not have the effect of limiting in any way the discretion of the Privacy Commissioner to deal as he or she sees fit with any Code Subscriber that is the subject of a complaint under this Code.

Revocation of Code Subscription

17. The Biometrics Institute Board shall notify the Code Administrator of its decision to revoke a Code Subscriber's subscription where:
17.1 a Code Subscriber fails to act in accordance with the final notice under subclause K.15; or
17.2 a Code Subscriber advises the Biometrics Institute Board by written notice to the Code Administrator that it wishes no longer to be a Code Subscriber.

Procedure upon Revocation

18. Upon revocation of the Code Subscription, the Code Administrator will:
18.1 notify in writing the Code Subscriber of the revocation, and, except in response to a advice under subclause K.17.3, set out the reasons for the revocation; and
18.2 remove the name of the Code Subscriber from the Public Register.

19. The steps referred to in subclause K.18 shall constitute deregistration of a Code Subscriber, and shall take effect from the date that the notification referred to in subclause K.18.1 is sent by the Code Administrator.

20. On receipt by the Code Administrator of a Code Subscriber's advice in accordance with subclause K.17.2, deregistration of that Code Subscriber will occur within seven (7) business days.

Federal Register of Legislative Instruments F2006L02406

21. On deregistration, the Code Subscriber must make no further representation that it complies with the Code.

Appeal

22. A Code Subscriber who has been deregistered in accordance with subclause K.18, may, within 7 business days of receipt of the notice referred to in subclause K.18.2, by written notice, appeal against the decision to the Chairperson of the Independent Code Review Panel.

23. The Chairperson of the Independent Code Review Panel shall give the deregistered Code Subscriber an opportunity to be heard and shall make a final determination.