Australian Government
Office of the Privacy Commissioner

Explanatory Statement

Approval of Biometrics Institute Privacy Code

This explanatory statement relates to an instrument made under s. 18BB(2) of the *Privacy Act 1988 (Cth)* (Privacy Act) entitled "Approval of the Biometrics Institute Privacy Code".

This explanatory statement has been drafted for the purpose of fulfilling the Office of the Privacy Commissioner's obligations under s. 26(1) of the *Legislative Instruments Act 2003* (Cth) (Legislative Instruments Act).

1. Purpose

The purpose of the instrument to which this statement relates is to grant approval by the Privacy Commissioner under Part IIIAA of the Privacy Act to the Biometrics Institute Privacy Code (the Code).

The Code commences on 1 September 2006.

2. Approved Privacy Codes

The *Privacy Amendment (Private Sector) Act 2000 (Cth)* extended the operation of the Privacy Act to cover much of the private sector. A feature of the Act is the option for organisations to develop their own privacy codes which, when approved, replace compliance with the National Privacy Principles (NPPs).

The co-regulatory approach adopted in the Act was developed on the basis that the privacy concerns of consumers can best be addressed if organisations are allowed room to develop an appropriate privacy standard with their customers. This approach ensures that an effective and comprehensive data protection framework is provided for the private sector in Australia while still allowing some flexibility in its application.

Section 18BA of the Privacy Act provides that "an organisation may apply in writing to the Commissioner for approval of a privacy code". "Organisation" is defined in s. 6C as any entity that is not a small business operator, a registered political party, an agency a State or Territory authority or a prescribed instrumentality of a State or Territory. A "small business operator" is defined in s. 6D as a business which has an annual turnover of $3 million or less and, subject to some exceptions, is exempt from the legislation.

Although a business may be exempt from the Privacy Act because it does not come within the definition in s. 6C, it may nevertheless choose to be treated as an organisation (see s. 6EA). In this instance, the Biometrics Institute has chosen to be treated as if it were an organisation.

The Code covers certain acts and practices in relation to code subscriber's employee records that would otherwise be exempt under the Act (as permitted by s.18BAA). Specifically, the Code covers certain of the acts and practices of employer organisations that are directly related to a current or former

employment relationship between the employer and individual, and directly related to an employee record relating to that individual held by that organisation. The Code applies 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. The aim of these provisions is to ensure that the 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 employee records which do not involve a biometric in the manner described in the Code remains exempt from the Code in accordance with s. 7B(3) of the Privacy Act.

The privacy rights of an individual cannot be lessened by the use of a code. For instance, the Commissioner must approve each privacy code in accordance with the Act. When deciding whether or not to approve a code, the Commissioner must consider whether the code incorporates all the NPPs or sets out obligations that, overall, are at least the equivalent of all the obligations set out in the NPPs.

Where an organisation consents to be bound by an approved code, the code operates in place of the NPPs until the organisation ceases to be bound by the code. Where an organisation chooses not to adopt an approved code it will be bound by the NPPs.

The Commissioner considers that periodic, independent reviews of a code and its operations are essential to the success of the co-regulatory regime. Such a requirement helps ensure that the code is meeting all the proposed objectives and remains relevant and up to date in a changing marketplace. The Code will be reviewed by the Biometrics Institute in three years.

3. Authority for approving a Privacy Code

An organisation may apply in writing to the Commissioner for approval of a privacy code under s.18BA of the Privacy Act. The authority for approving a code is governed by s. 18BB which reads:

> **s. 18BB Commissioner may approve privacy code**
>
> (1) Before deciding whether to approve a privacy code, the Commissioner may consult any person the Commissioner considers appropriate.
>
> (2) The Commissioner may approve a privacy code if, and only if, the Commissioner is satisfied:
>
> (a) that the code incorporates all the National Privacy Principles or sets out obligations that, overall, are at least the equivalent of all the obligations set out in those Principles; and
>
> (b) that the code specifies the organisations bound by the code or a way of determining the organisations that are, or will be, bound by the code; and
>
> (c) that only organisations that consent to be bound by the code are, or will be, bound by the code; and
>
> (d) that the code sets out a procedure by which an organisation may cease to be bound by the code and when the cessation takes effect; and

(e) of the matters mentioned in subsection (3), if the code sets out procedures for making and dealing with complaints in relation to acts or practices of an organisation bound by the code that may be an interference with the privacy of an individual; and

(f) that members of the public have been given an adequate opportunity to comment on a draft of the code.

The approval by the Privacy Commissioner of a privacy code has the effect of altering the content of the law. As a consequence, the written approval of a privacy code under s. 18BB(2) of the Privacy Act is a legislative instrument for the purposes of the *Legislative Instruments Act 2003.* However, the approval instrument is not subject to disallowance as it is exempted by Schedule 2 of the *Legislative Instruments Regulations 2004*.

4. Reasons for approving the Code

The Privacy Commissioner is satisfied in accordance with s.18 BB(2)(a) of the Privacy Act that the Code incorporates all the NPPs. NPPs 1 to NPP 10 have been included in the Code without changes to their substance. The Code also incorporates higher standards of privacy protection than the NPPs require in the following principal areas:

- The approved Code covers certain acts and practices in relation to employee records that otherwise would be exempt (see above). Specifically, the Code covers the acts and practices described in clauses D.4 and D.5 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.
- The inclusion of Supplementary Biometrics Institute Principles 11, 12, and 13 in the Code:
  - Principle 11 deals with the protection of biometric information and in some ways supplements the data security obligations in NPP 4.
  - Principle 12 includes some added notice requirements, restricts some secondary uses without express free and informed consent and confers a right to request the removal of biometric information from a system. These obligations enhance NPP 1.3, NPP 1.5, NPP 2 and NPP 4.
  - Principle 13 introduces an obligation of accountability through an extra notice obligation, requires an audit of biometric systems to be undertaken, introduces the concept of holistic privacy management in relation to a biometric product or service, and mandates the use of privacy impact assessments. These requirements augment NPP 1, NPP 4 and NPP 5.1.
- The inclusion of a specific requirement in item “G. Standards” in the Code for code subscribers to be aware of and take account of relevant national and international standards for information protection and biometric systems.

The Privacy Commissioner is also satisfied in accord with s. 18BB(2)(b), (c), (d), and (f) of the Privacy Act that the following matters are adequately addressed in the Code:

- The Code specifies a way of determining the organisations that are, or will be, bound by the Code.[1]
- That only organisations that consent to be bound by the Code are, or will be, bound by the Code.[2]
- The Code sets out a procedure by which an organisation may cease to be bound by the Code and when the cessation takes effect.[3]
- That members of the public have been given an adequate opportunity to comment on the draft of the Code.[4]

As the Code does not set out procedures for making and dealing with complaints in relation to acts and practices of an organisation bound by the Code that may be an interference with the privacy of an individual, the Privacy Commissioner was not required to consider whether s.18 BB(2)(e) of the Privacy Act has been satisfied.

The Code provides that the Privacy Commissioner is the complaints adjudicator and as such is bound by the provisions of Part V of the Privacy Act regarding procedures for receiving and dealing with complaints.

5. Consultation

The Code was developed by the Biometrics Institute in consultation with its members and members of the public.

The Privacy Commissioner has not been directly involved in consultation with respect to the approval of the Code. However, under section 18 of the Legislative Instruments Act there are certain circumstances in which a rule-maker may be satisfied that consultation is unnecessary or inappropriate. Section 18(2)(e) provides that one such circumstance is where appropriate consultation has already been undertaken by someone other than the rule-maker.

The Privacy Commissioner was advised that consultation in relation to the draft of the Code by the Biometrics Institute involved the following procedures:

- Consultation on the form, structure and content of the draft Code commenced in April 2003 followed by a round of stakeholder meetings to identify key issues. These issues were canvassed more widely in a discussion paper released by the Biometrics Institute in 2003. Comments on the draft Code were received and it was revised accordingly.
- Over 800 individuals participated in meetings, workshops and via written submissions. The views of privacy advocates were represented

[1] See "C. APPLICATION" and "K. REGISTRATION AND DEREGISTRATION" in the Code.
[2] See "C. APPLICATION" item C.3 and "K. REGISTRATION AND DEREGISTRATION" in the Code.
[3] See "K. REGISTRATION AND DEREGISTRATION" K.17 and K.18 in the Code.
[4] See "5. Consultation" below.

mainly by the Australian Privacy Foundation and the Australian Consumers Association although many other non-industry stakeholders provided input.

- Consultations occurred with various groups throughout 2003, 2004 and 2005 including with focus groups. Refresher consultations were undertaken during 2006 by the Biometrics Institute.
- Public awareness of the Code has been assisted by an announcement on the Office of the Privacy Commissioner's web site together with a link to the Biometrics Institute's web site. The Biometrics Institute's web site contains comprehensive information on the Code together with access to the relevant documentation. This web site information has been in place since December 2003.

As a result, the Privacy Commissioner is satisfied that an appropriate level of consultation has been undertaken to comply with the requirements of the Legislative Instruments Act.

The Privacy Commissioner is also satisfied that the consultation undertaken was adequate to satisfy the requirements of s. 18BB(2)(f) of the Privacy Act which requires that members of the public have been given an adequate opportunity to comment on the draft of the Code.