Annex D

to APF Submission to Senate Legal & Constitutional Committee Inquiry into the Privacy Act 1988, March 2005

Biometrics Institute Draft Privacy Code of Practice

Submission by the Australian Privacy Foundation

March 2004

The Australian Privacy Foundation

The Australian Privacy Foundation (APF) is the main non-governmental organisation dedicated to protecting the privacy rights of Australians. The APF aims to focus public attention on emerging issues which pose a threat to the freedom and privacy of Australians. The APF has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions. The APF uses the Australian Privacy Charter as a benchmark against which laws, regulations and privacy invasive initiatives can be assessed. For information about the APF and the Charter, see www.privacy.org.au

Overview – purpose and status of Code

We commend the Institute for its work and extensive consultations. There is clearly considerable value in giving guidance on how privacy principles apply to the collection and use of biometrics, and we can also see value in Institute members committing themselves to higher standards than are required by law, in order to gain public confidence in this sensitive privacy area.

We accept that biometrics can be both privacy enhancing, eg: when used to provide security against unauthorised access to other personal information; and privacy intrusive, eg: when used to monitor an individual's movements or activities. Striking an appropriate balance is likely to be one of the major challenges of privacy regulation as the use of biometrics becomes more widespread.

We agree with all of the reasons for developing a Code (paragraph 6) except for the obviation of regulatory intervention, which we regard as almost certainly necessary and justified for at least some aspects of biometrics.

However, we are not convinced that it makes sense to seek registration of a Code of Practice under Part IIIAA of the Privacy Act. Any Institute member signing up to a registered Code would effectively be accepting replacement of their obligations under the National Privacy Principles (NPPs) with those in the Code (largely the same but with some changes and additions). However, many Institute members and others who might be interested in adopting the Code standards are *not* subject to the NPPs – these include Commonwealth government agencies (subject to the IPPs) state government agencies (subject to various state laws or administrative privacy principles), and overseas government agencies (eg NZ) subject to their own laws or codes. It would make no sense for any of these bodies to sign a Code which has formal status only for private sector organizations in Australia.

Also, even for those signatories who are bound by the NPPs, the Code would only apply to a small part of their full range of activities. Any activities that did not involve the use of biometrics would remain subject to the NPPs, and it is difficult to see how a clear distinction could be drawn in most biometric applications. There would be great potential for confusion and dispute about whether a particular act or practice was subject to the Code or the NPPs. We believe in general that 'horizontal' Codes such as this are not suitable for registration under the Privacy Act, whereas 'vertical' Codes applying to all the activities of particular industry sectors may be suitable. This is one of the main reasons why, for instance, banks have neither developed a banking privacy code nor signed up to the registered General Insurance Privacy Code.

As an alternative, we recommend that the Institute offers the guidance to members and others as an unregistered Code, which is equally applicable to all organizations which are either required to, or wish to, follow the common privacy principles underlying all privacy laws and codes.

Even though unregistered, the Code can still be voluntarily binding on adopters, with signatories agreeing to be held accountable for complying with its provisions. This would however require the Institute to establish a complaints handling and dispute resolution mechanism, since the Privacy Commissioner could not take on this role.

While there is some attraction in the Code's additional protections being enforceable in law, we believe that this is outweighed by the likely deterrent effect on the rate of adoption. In the interests of attracting as many relevant organizations as possible to adopt the Code, we favour leaving them as voluntary guidelines.

Content of the Code

The Code largely replicates the wording of the NPPs. This is unexceptional, although as we have argued above, redundant.

If the Institute persists with the Code as a complete replacement for the NPPs, then all the elements of the NPPs must remain – including NPP 2.1(c) which has been excluded on

the grounds that it is not relevant to biometrics. This misses the point – if signatories are to adopt the Code it must cover the same ground as the NPPs – a Code cannot 'cherry pick' other than to improve the level of protection – it must under Part IIIAA contain obligations that are 'overall, at least the equivalent' of the NPPs.

We focus our remaining 'content' comments on the additional obligations introduced by the draft Code and on further additional obligations which we consider could usefully be included. Most of these can and should be related back to one or more of the NPPs, as follows.

Eligibility (Section C- but see also registration in Section K)

The criteria for 'eligibility' to become a Code Subscriber (and for ineligibility) are not stated, other than the requirement to be an Institute member. Other criteria will presumably include some connection with biometrics either as a supplier or user. It would be helpful (not least to potential applicants) for the criteria to be spelt out. We cannot see why the Institute could not allow non-members to be subscribers to the Code – depending on the financial model adopted this could help to spread the cost of Code administration, and many organizations may find it easier to justify subscription to the Code than membership of a representative body which takes policy positions and lobbies.

Terminology (Section D)

The two sets of definitions should be rationalised and all those which are taken directly from legislation should be clearly identified as such.

'Biometric' needs to be defined more clearly and precisely. The current definition is simply wrong – not all biometrics are unique, and they can be used for other purposes than identification – for instance a biometric access control system can simply authenticate users without identifying them. A critical issue is whether a biometric has to be derived. Digital photographs are arguably a biometric in themselves, even without further analysis by face recognition software. Are fingerprint images a biometric, or only the code used to describe a fingerprint under accepted international standards?

Collection of biometrics takes place at both enrolment and verification stages, and both should be given equal recognition in the definition.

Principles (Sections E & F)

Collection

The provision for privacy impact assessments (Code 13.4) belongs under collection as it should be a necessary precursor to any collection and subsequent use. It is a specific way of satisfying 'justification' and 'proportionality' privacy principles such as NPP 1.1 and IPP 1.1(b) in the Privacy Act 1988 (Cwth).

There should be some reference to minimum standards for the conduct of privacy impact assessments – there are several models available including the New Zealand Privacy Commissioner's Privacy Impact Assessment Handbook, and PIA Guidelines issued by the Australian federal Privacy Commissioner in relation to Public Key Infrastructure.[1]

Proposed principle 12 - control – is welcome – voluntary participation (12.1) is a valuable threshold to be crossed before any collection can take place (other than where required by law). It would however be useful to explore the practical implications of this principle – for instance the extent to which consent for participation needs to be both free and fully informed. The ability to revoke consent and withdraw from participation (12.3) is obviously a good indicator of consent being truly free, but as 12.3 recognises, withdrawal may not always be practicable.

A related issue – raised in the Discussion Paper (DP 9.11) but not followed up in the Code is conscientious objection – there should be an obligation for any application of biometrics to address this, and also to not unreasonably discriminate against any particular segment of the affected population – eg; persons with disabilities, ethnic minorities.

The Code could usefully make a distinction between overt and covert collection of biometrics. Following the model of existing surveillance legislation, overt collection (with knowledge of the subject) should follow all parts of the Code. Covert collection (ie without knowledge of the subject) should require a judicial warrant as the only authority for collection (replacing consent and other grounds in the collection principle), as well las compliance with all the other relevant principles (some modification of the openness and access and correction principle would be required).

Use and disclosure

The Code could usefully include limitations on secondary uses for unrelated analysis – particularly of any health related characteristics. It has been suggested that various biometrics can be indicative of physical or mental state, such as stress levels, or even actual conditions (iris scanning). There should be a presumption that any secondary analysis of biometrics collected for purposes such as authentication or identification is not permitted without express free and informed consent (or at all).

[1] As well as from several North American jurisdictions

Data Quality

The Code could usefully address issues of data quality that are specific to various biometric systems such as the 'uniqueness' of different biometrics and the incidence of false positives and negatives with particular applications.

Security and storage

Most of the additional provisions under the new 'protection' principle 11 of the Code are in effect supplementary guidance on compliance with the Security principle (4), and in our view should be clearly linked to this principle.

11.1 Encryption should certainly be considered and is likely to be justified for many biometric systems but we are not convinced it need be mandatory. There is also the question of what strength of encryption is appropriate. We support the inclusion of a recommendation to use encryption of appropriate strength where justified as a security measure.

11.2 We are not persuaded that a simplistic requirement for 'separation' is helpful – the objective apparently underlying this provision is sound, but may need to be realised in a variety of ways.

11.6 Records should show which individuals have had access to *which* biometric data, *on which occasions* – ie: there should be detailed audit trails, where appropriate.

The Code could usefully address the issue of where the biometric is stored and in what form. For those biometrics derived from an image (eg: of a fingerprint or face), there is the question of whether the image itself needs to be retained at all once a biometric measurement has been taken. A related question is whether it is possible to reconstruct an image (or other facsimile) from the biometric – if so there are obviously additional security implications. Another important issue is whether the master template is stored in a central database or only needs to be on a token held by the user (such as an identity card). Storage on a central database not only raises security issues but increases the potential for secondary uses (function-creep or scope-creep).

Openness

The requirements for express notification of purposes (13.1); for notification of changes to scope or purpose (12.2) and for 'not misleading' (13.5) are helpful expansions of the notification requirements of Principle 1 and of Principle 5.

The Code could usefully require the publication of statistics on false positives and false negatives in biometric applications – only with transparency on this key performance indicator can the public assess whether the claimed benefits of any particular application

are realised and whether the 'price' is too high in terms of false assurances and inconvenience or worse for those wrongly 'rejected'.

The discussion paper raised the important issue of whistleblower protection (DP 9.9 & 9.12) – the Code should provide for adequate protection of employees or others who disclose breaches of the Code or other public interest matters.

Auditing

The requirement for auditing (13.2) is welcome, and could partly be seen as necessary in respect of security measures to satisfy Principle 4. The Code should however include more detail on the scope of audits (compliance with all principles) and standards (of independence, professional competence) etc. Consideration could be given to a system of accreditation for auditors of biometric systems.

Responsibility for holistic end-to-end view

This aspirational provision (13.3) may be too unrealistic and unduly onerous to form an enforceable part of any Code. Various players in the supply chain for any biometric system will realistically often have only limited ability to influence wider policy decisions. We suggest that this requirement is re-cast as a responsibility to consider and draw attention to privacy management issues.

Complaint Handling (Sections J and implications for Section H)

In its draft Code the Institute has chosen not to establish a Code Adjudicator, leaving complaints not resolved by the respondent organization to be resolved by the Privacy Commissioner.

Given the well-publicised resource constraints on the Office of the Federal Privacy Commissioner (OFPC) we suggest that the Institute could add significant value by providing through the Code an 'industry' dispute resolution mechanism, provided it could offer consumers significant time or cost advantages over relying on the OFPC.

If the Code was registered under the Privacy Act a dispute resolution mechanism would have the status of a Code Adjudicator, offering an intermediate level of external dispute resolution between the internal procedures required under Section J and the right of appeal under the Act to OFPC.

If our earlier recommendation is followed and the Code is not registered, but remains a voluntary industry scheme, it could still usefully include an external dispute resolution mechanism.

The proposed Code Review Panel could be given the dispute resolution function as well, as the criteria for establishing such a mechanism, under the *Benchmarks for Industry-Based Customer Dispute Resolution Schemes*, August 1997 (**t**he DIST Benchmarks), are very similar.

Both the internal and any external dispute resolution mechanisms should follow Standards Australia 4269 (AS4269)[2].

Remedies

Because the draft Code defers to the Privacy Commissioner's complaint processes, it does not address the question of appropriate remedies. In our view, the Code should recognise the principle that consumers should be compensated for failures in biometric technologies, and that compensation should be proportional to the loss or damage caused by the failure. If the Code establishes an external dispute resolution mechanism, it will need to go into the issue of remedies and compensation in more detail.

Review (Section I)

The Code Review Panel (whether or not it takes on an additional complaints function as recommended above) should include equal numbers of consumer and industry representatives, as well as the independent chair. Consumer representatives should be chosen from a short list nominated or approved by a consumer peak organization – we suggest the Consumers Federation of Australia, which now performs this 'recruitment' function for a wide range of consumer representative appointments, and has a published policy on consumer representation. See http://www.consumersfederation.com/representation.htm

Paragraph I 3.2 implies that the Panel will be a standing body, ie: not just constituted for the purposes of the reviews – this is commendable and has implications for the improper conduct provisions in section K (see below).

Registration (Section K)

See comments on eligibility under Section C.

The function of judging 'seriously improper conduct' (K.13) would sit better with the Code Review Panel rather than the Institute Board, to ensure independence and avoid any conflict of interest. This would however mean that the Panel could not fairly also hear

[2] AS4269-1995, *Complaints Handling*.

appeals under K.22-23. We are not convinced that an appeal stage is necessary if the initial assessment was by the independent panel.

The reference in K.16 to the discretion of the Privacy Commissioner to deal with Code subscribers should not be limited to 'subscriber[s] that [are] the subject of complaint' – the Commissioner may also deal with subscribers through an 'own-motion' investigation under s. 40(1)(a) of the Privacy Act, without any complaint having been made.

We are not sure why K.17.2 is necessary as in these circumstances sections K.13-15 would have applied – and K.17.1 already covers this. It would however be desirable to build consultation with the Privacy Commissioner into K.17.1.

Australian Privacy Foundation
30 March 2004

Contact:

****
Nigel Waters, Board Member
Australian Privacy Foundation
http://www.privacy.org.au
Tel: (02) 4981 0828 or Mobile: 0407 230 342
Fax: (02) 4981 0995
nigelwaters@iprimus.com.au
****