Australian Privacy Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

6 November 2015

Mr S. Corbell MLA
Attorney-General
ACT Government

Cc: Mr T. Pilgrim, Privacy Commissioner
Mr W. Rowlings, Secretary, Civil Liberties Australia

Dear Mr Corbell

Re: National Facial Recognition Database

The Australian Privacy Foundation (APF) notes the reports in at least The Guardian, The Canberra Times, itNews and two biometrics industry outlets about the concerns you have raised regarding the proposed national facial recognition database.

APF further notes that you are reported to have opposed the measure because of the "significant privacy and human rights concerns that have not been satisfactorily addressed" and the inadequacies in the privacy impact assessments.

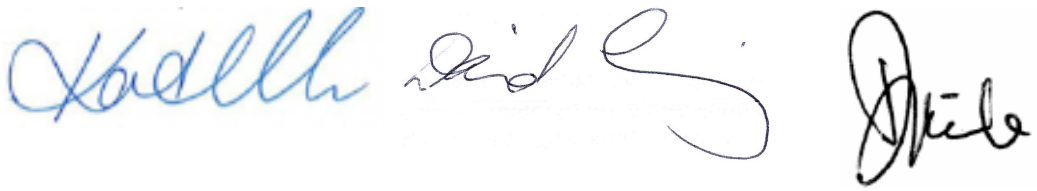
APF strongly supports your position on this matter.

APF urges you to sustain your opposition to the proposal in the face of the pressure that national security agencies and technology providers are likely to bring to bear. We believe that many people are very disturbed about the accumulation of personal images from a wide variety of sources, most of them captured for purposes very different from those that the government has in mind.

In support of your position, we attach copies of the APF Position Statements on PIAs and Biometrics.

We continue our work to encourage members of parliaments around the country to appreciate and speak out about the serious and unjustified harm to privacy and human rights that such schemes embody.

Yours sincerely



Kat Lane, Vice-Chair
0447 620 694
Kat.Lane@privacy.org.au

(Dr) David Lindsay, Vice-Chair
(03) 9905 5547
David.Lindsay@privacy.org.au

David Vaile, Vice-Chair
0414 731 249
David.Vaile@privacy.org.au

APF Policy Statement on Privacy Impact Assessments

Privacy Impact Assessment (PIA) is a systematic process that identifies and evaluates, from the perspectives of all stakeholders, the potential effects on privacy of a project, initiative or proposed system or scheme, and includes a search for ways to avoid or mitigate negative privacy impacts.

This Policy Statement comprises the following sections:

PIA compared with Other Business Processes

A PIA differs from other privacy-related business processes, in the following ways:

Activities Conducted Prior to a PIA

- **Privacy Strategy Formulation**. This process considers privacy from a corporate perspective; whereas a PIA considers it from the perspectives of all stakeholders, and focusses on a particular initiative, scheme, program or project. In this Policy Statement, the term 'project' is used to encompass all such categories of activity
- **Privacy Issues Analysis**. This process is a preliminary, internal assessment of the potential issues that may arise from a project, and is generally undertaken at a very early stage in the project life-cycle; whereas a PIA is performed at greater depth, and through the project life-cycle, and involves engagement with stakeholders
- **PIA Screening Study, or 'Threshold Assessment'**. This process is an initial, 'broad-brush' survey, which is undertaken early in the project life-cycle in order to determine whether a PIA needs to be performed, and if so what scope the PIA should have; whereas a PIA is an in-depth assessment of privacy impacts

Activities with Narrower Scope than a PIA

- **Data Privacy Impact Assessment**. This process is a study of the impacts of a project on only the privacy of personal data; whereas a PIA considers all dimensions of privacy
- **Internal Cost/Benefit Analysis**. This process is an assessment of the costs and benefits of a project from the viewpoint of the organisation alone, and is often limited to financial costs and benefits; whereas a PIA adopts a multi-perspective approach, taking into account the interests of all stakeholders, and considers costs and benefits of all kinds, not just those that have measurable financial impact
- **Internal Risk Assessment**. This process is an assessment of the risks arising in relation to a project from the viewpoint of the organisation alone; whereas a PIA adopts a multi-perspective approach, taking into account the interests of all stakeholders
- **Privacy Impact Statement**. This process is a declaration by the organisation; whereas a PIA is a process
- **Legal Compliance Assessment**. This process is an assessment of the extent to which the project complies with relevant laws; whereas a PIA assesses a project against the needs, expectations and concerns of all stakeholders

Activities Conducted Subsequent to a PIA

- **Privacy Policy Statement (PPS)**. This is a declaration of the organisation's undertakings in relation to privacy; whereas a PIA is a process used to establish what undertakings need to be given
- **Privacy Management Planning and Control**. This is a systematic process of ensuring that a Privacy Management Plan is articulated and implemented, and its performance monitored, in order to give effect to the privacy-relevant decisions made during the project; whereas a PIA is the process that identifies the problems, and identifies solutions to them
- **Privacy Audit**. This process is an assessment conducted after a project is implemented; whereas a PIA is conducted before and in parallel with a project, and ensures that harmful and expensive problems that an audit would later expose are avoided, and that unavoidable negative impacts on privacy are minimised and the harm mitigated

Characteristics of a PIA

In order to fulfil its purpose, a Privacy Impact Assessment process needs to have all of the following characteristics.

1. Purpose of the PIA

From the perspective of people whose privacy may be negatively affected by a project, the PIA's purpose is to ensure that the projects's impacts and implications are understood prior to implementation, and that unnecessary negative impacts are avoided or that mitigating measures are in place.

From the perspective of the sponsoring organisation(s), the PIA's purpose is to enable the organisation and its partners to appreciate privacy concerns, to avoid or mitigate negative privacy impacts and implications, and to do so at a sufficiently early stage in the project life-cycle that costly re-work and feature retro-fit are avoided.

2. Responsibility for the PIA

The responsibility for the conduct of a PIA rests with organisations that sponsor, propose or perform projects that have the potential to negatively impact privacy.

In many cases, external expertise will be acquired under contract, because few organisations would find it appropriate to invest in full-time employees who already had, and could sustain, up-to-date knowledge in such a specialised area. In addition, an appropriate consultant can provide access to external perspectives that may otherwise be difficult for the organisation to appreciate. However, merely delegating the conduct of the PIA to an external contractor does not satisfy the requirements. Similarly, an assessment undertaken by a regulatory or oversight agency is not a PIA, but rather a form of accountability and external control.

Within the sponsoring agency, governance arrangements are necessary, to ensure that:

- responsibility for the PIA rests with an appropriate senior executive
- relevant staff are involved, and commit sufficient time to the process
- the organisation has intellectual ownership of the process and the information arising from it
- the information arising from the process is assimilated and internalised rather than walking out the door when consultants leave
- the conclusions reached are articulated forward into the design rather than lying dormant in the PIA Report

3. Timing of the PIA

The PIA must be commenced sufficiently early that information arising from it is fed forward into the design process. If that is not the case, then there is a considerable risk that the design will have undue negative privacy impacts, and that re-work and feature retro-fitting will be necessary. This creates project risk, and gives rise to delays and to much higher costs than is the case where an in-depth understanding of privacy concerns is factored into the design process from the outset.

Where a project is large or long, the PIA process needs to be multi-phased, commencing at project initiation or at least during the requirements analysis phase, and running in parallel and inter-leaved with design, implementation and deployment.

4. Scope of the PIA

A PIA process has to have sufficient scope. Three aspects are particularly crucial to a successful undertaking.

• The Dimensions of Privacy

A PIA process must not be limited to data/information privacy, i.e. the protection of personal data. Other categories of importance are:

- privacy of the physical person
- privacy of personal behaviour
- privacy of personal communications.

• Stakeholders

The perspectives of all stakeholders must be reflected, not merely those of the sponsor(s) and its/their strategic partners. In particular, the scope of the stakeholder notion must include:

- the categories or segments of individuals whose privacy is or may be affected by the project
- representative associations and advocacy organisations for the interests of the categories or segments of individuals whose privacy is or may be affected by the project

Stakeholder Analysis needs to be undertaken in order to identify the categories of entities that are or may be affected by the

project, and whose actions may affect the success of the project

• Reference-Points

A PIA process must of course take into account laws relevant to privacy. This may include one or more privacy or data protection statutes, but it also includes many other pieces of legislation that provide incidental protections or that establish privacy-relevant regulatory requirements, and, in common law jurisdictions, torts (such as confidentiality) and case law. In the case of government agencies and government business enterprises, their own enabling and/or governing legislation generally also contains privacy-relevant requirements.

However, the reference-points used in identifying negative privacy impacts need to be much broader than just the applicable laws. There are many public needs, expectations and concerns that are felt by individuals, categories of individuals and communities that may not be (or may not yet be) reflected in law. A PIA process that overlooks these aspects will result in a design that earns opprobrium from advocacy organisations and the affected public. Hence, despite being legally compliant, schemes will encounter resistance, and be the subject of complaints and negative media coverage.

5. Stakeholder Engagement

The PIA process must include meaningful engagement by the sponsoring organisation with all stakeholders. For meaningful engagement to be achieved, all of the following are necessary:

- early contact with all stakeholders and notification of the nature of the project
- information provision, to enable stakeholders to consider the proposal and formulate their views
- consultative processes,such that stakeholders can seek clarifications, and communicate their views
- sufficiently early conduct of consultation that the outcomes can be fed forward to and reflected in the design, rather than the PIA Report arriving after the key design decisions have been made and changes have become costly
- interactions among stakeholders, in order to overcome barriers to communication, avoid misunderstandings, develop shared appreciation of the aims and constraints, and enable participants to work together towards constructive outcomes
- communication to participants of a summary of the process and outcomes
- exposure to participants of the draft PIA Report
- publication of the final PIA Report, to ensure that the public is informed, and as a means of supporting accountability

Some organisations may be concerned about the exposure of information of commercial or competitive value or security-sensitivity, and others about the disclosure of information that is subject to constraints, e.g. because no Cabinet decision has yet been made. It is necessary to reconcile the need for meaningful engagement with the affected public against such security and confidentiality limitations.

6. Orientation

The PIA process needs to have appropriate orientation.

• Process vs. Product

The PIA needs to be clearly and consistently depicted as being primarily about process. If, on the other hand, a PIA is projected or perceived as being merely a formal procedure that produces a PIA Report, then the project will fail to achieve the insights, understanding, behavioural change and business process features that an effective PIA process leads to.

• Solutions vs. Problems

PIA is a form of risk management. This means that it goes beyond 'problems', 'issues' and 'concerns', and extends to a search for 'solutions'. More specifically, it involves active search for means of avoiding negative privacy impacts wherever that can be achieved, and for means of mitigating the negative impacts where avoidance is not feasible.

7. The PIA Process

A preliminary privacy issues analysis process enables projects to be screened, and threshhold tests applied, in order to determine whether a PIA is necessary, and, if so, what the scope of the assessment should be.

The PIA process as a whole needs a degree of structure, such as a preliminary phase, followed by preparatory, performance, documentation and review phases.

Considerable benefits can be gained from integration of the PIA process into relevant corporate processes, such as project funding, project approval, risk management, project management and internal review mechanisms.

PIA guidance documents offer considerable value in planning and performing the process; but they need to be applied intelligently rather than being thought of as a recipe, and checklists need to be recognised as not necessarily being sufficiently comprehensive to support the assessment of any particular project.

8. Outcomes from the PIA Process

The documents that are produced by the PIA process importantly include the following:

- a PIA Report. This documents the process and its results
- a Privacy Management and Control Plan. This documents the problems, and how they are to be addressed, including the specific design features that achieve avoidance or mitigation of each specific negative privacy impact

The outcomes derive from the implementation of the Privacy Management and Control Plan. They importantly include the following:

- insights, understanding and behavioural change
- design features
- minimal negative privacy impacts on individuals
- achievement of the sponsoring organisation's aims in an effective and efficient manner, without attracting negative media coverage, and with the support of (or at least without unreasonable opposition by) the relevant public, and representatives and advocates for their interests

---

Guidance Documents Published by Australian Privacy Commissioners

The Australian Privacy Commissioner

The Commonwealth Commissioner published a PIA Guide 2006. There has been one subsequent revision (OAPC 2010).

In general, much of that document provides valuable guidance; but unfortunately it suffers from several critical deficiencies, which the Privacy Commissioner has declined to address. These are:

- consultation is entirely omitted from the description of the PIA process
- there is no mention of the role of representatives and avocates for affected population segments
- the orientation is strongly towards impacts and issues, with far less attention paid to solutions
- although mention is made of the need to avoid harm to privacy, no mention at all is made of mitigating measures

The Victorian Privacy Commissioner

Since the revisions made to its original 2004 document, the guidance document published by the Victorian Privacy Commissioner (OVPC 2009a) is one of the best such documents published anywhere in the world.

Its one disadvantage in that it structures and describes the PIA process in terms of the preparation of the PIA Report - which risks readers thinking of a PIA as a mere product rather than primarily a process. On the other hand, the Template (OVPC 2009b) and the Accompanying Guide (OVPC 2009c) draw the assessor well beyond mere legal compliance, place considerable emphasis on consultation and solution-orientation, and provide instruction without permitting the assessor to abandon intellectual engagement with the work.

APF thanks its site-sponsor: Hosted by GoWeb®

This web-site is periodically mirrored by
the Australian National Library's Pandora Archive
and by the Wayback Machine since March 2000

Created: 11 March 2013 - Last Amended: 11 April 2013 by Roger Clarke - Site Last Verified: 11 January 2009
© Australian Privacy Foundation Inc., 1998-2015 - Mail to Webmaster

Biometrics

Original Version of 5 April 2008 – Amended 15 October 2011

Summary

Technology providers are trying to sell biometrics schemes, and some organisations are buying them, without regard for the security and privacy of the people the schemes are being imposed upon. Now even school-children are being trained to submit to biometric measurement, and to accept physical intrusions and continual techno-surveillance as part of their lives.

This document expresses the APF's policy in relation to biometrics.

The APF's policy is that all biometric schemes must be the subject of a moratorium.

No new biometric schemes should be implemented until and unless comprehensive laws have been brought into effect to regulate them.

Each proposal must be demonstrated to be justified, must be subject to a Privacy Impact Assessment (PIA), including consultation with the affected people and their representatives and advocates, and must include appropriate safeguards. It will then be essential to review existing applications of biometrics, to ensure that they also measure up against the standards.

Background

A biometric is a measure of some physical or behavioural attribute of a person, which is intended to be unique, or at least sufficiently distinctive to assist in recognising who the person is.

Few if any biometrics are actually unique; but technology providers promote the myth that they are, and user organisations happily believe it. A great many biometric schemes have been invented, and many have failed and disappeared. Those currently in the market include fingerprints and iris scans (which under ideal conditions can produce some degree of reliability), hand geometry and voice scans (which under ideal conditions can be of some use in authenticating whether the person is who they purport to be), and so-called 'face recognition' technologies (which not only do not 'recognise faces', but are not even based on any attribute that could give rise to reliable distinctions between different people).

The most common form of biometric scheme involves a 'reference measure' being acquired for each person, together with an identifier such as their name, and stored somewhere. Subsequently, 'test-measures' can be compared against one particular reference measure, or against multiple reference measures.

For a great many reasons, the measurements are always inaccurate, and the matching is always 'fuzzy'; so results ought to be expressed as probabilities. But that is administratively inconvenient, so most biometric systems just determine a Yes/No result, based on some arbitrary threshold. The thresholds are set and adjusted pragmatically, in order to achieve a compromise between generating large numbers of 'false positives' (unjustified suspicions), on the one hand, and large numbers of 'false negatives' (failures to find what should have been matches), on the other.

Biometrics can be used for authentication. In this case, a test-measure is compared against a reference-measure for a particular person, and the decision is either that the person is accepted as being the right one, or rejected. Alternatively, biometrics can be used for identification, in which case the test-measure is compared against the reference-measures of large numbers of people. Authentication uses are error-prone, and in some cases such as 'face recognition', highly error-prone. Identification uses are highly error-prone, in some cases such as 'face recognition', hugely error-prone.

Biometrics have been implemented or proposed as a basis for forensic evidence in law enforcement and some civil cases, for identifying people at border-crossings, for controlling access to secure areas, for checking that a token (such as a passport or credit-card) is being presented by the person it was issued to, and for recording attendance (e.g. by people on parole, or on remand, but also for employees and even school-students).

APF POLICY re BIOMETRICS

1. Biometrics are Extraordinarily Privacy-Invasive

Biometrics invade the privacy of the physical person, because they require people to submit to measurement of some part of themselves. In many circumstances, people are required to degrade themselves, and submit to an act of power by a government agency or corporation, e.g. by presenting their face, eye, thumb, fingers or hand, or having body tissue or fluids extracted, in whatever manner the agency or corporation demands. This may conflict with personal beliefs and customs.

Biometrics invade the privacy of personal behaviour, because they are a key part of schemes that provide government agencies and corporations with power over the individual. That not only acts as a deterrent against specific undesirable behaviours, but also chills people's behaviour generally.

Biometrics invade the privacy of personal data, because biometric measurements produce highly sensitive personal data, and that data is then used, and in many cases stored and re-used, and is available for disclosure, e.g. by the Australian government to other governments, including U.S. immigration and national security agencies.

2. Biometrics are Highly Error-Prone and Unreliable

Biometric schemes try to impose rigid technology on soft human biology, and in enormously varying contexts. Among many other challenges, the nominally unique features are mostly three-dimensional, and vary over time, and hence it is simply not feasible to 'capture' a representation of the features into digital form in a consistent manner. The equipment has to cope with many different environmental conditions (such as the strength and angle of light, the humidity, the temperature, and the dust-content in the air). In addition, it is impossible to ensure that manual procedures are performed in standard, invariant ways by lowly-paid security staff.

The comparisons performed between measures ignore all of the subtleties and reach a decision that is more or less arbitrary. A proportion of people (somewhere between 2% and 5%, or between 400,000 and 1 million Australians) are 'outliers' whose measures will always be highly problematical (e.g. because their fingerprints are faint, or worn down). A further serious problem is that many people accept the imposition nervously, sullenly or uncooperatively, and some actively resist it and seek to subvert it – some of them with serious criminal intent, but others without it.

As a consequence of these problems, there are a great many sources of error. That in turn means that tolerance-ranges have to be set quite high. Errors that are 'false-negatives' mean that the system doesn't achieve its primary objective. False-positives, on the other hand, give rise to wrongful suspicions, create considerable anxiety for the people concerned, and deflect organisational focus and resources away from more effective security measures.

3. Biometrics are Highly Insecure

An individual or organisation that acquires a person's biometric can use it to commit identity fraud or outright identity theft, and to 'plant ' false evidence.

Biometric technologies are commonly able to be subverted in order to produce an 'artefact'. That enables a person to masquerade as someone else.

If a person's biometrics are compromised by someone else, they cannot be revoked. So the risk of 'biometric theft', which exists for everyone, lasts their whole life long. Hence, even if it makes sense to use biometrics for a very small number of really important purposes, it doesn't make sense to undermine such reliability as it has by using it for trivial applications.

4. Biometrics assist Identity Fraudsters and Thieves

Far from solving masquerade and identity theft, biometrics are actually part of the problem.

Biometrics technologies are opaque. Organisations don't understand them, but instead just assume that they work, without conducting continual tests to ensure that they are still functioning as they were intended to, and haven't been neutralised. So masquerades that subvert biometric technologies are highly unlikely to be detected.

Added to that, many biometric schemes involve reference-measures and test-measures being exposed in the data-gathering equipment, networks, intermediate storage and long-term storage. Particularly in long-term storage, the data is highly attractive, and it is impossible to prevent unauthorised uses, and 'function creep' to new purposes.

5. Biometrics Errors impose Serious Risks on Powerless People

Biometric schemes are imposed on people by powerful organisations. In most cases, no meaningful consent is involved. Yet the large numbers of failures to capture a usable measure and the many false-positives impact the affected individuals much more than they do the scheme's sponsor. Everyone who is subject to such errors suffers at least inconvenience and embarrassment. Much more serious problems are created for some people, who may be falsely accused of misbehaviour or crime, unjustifiably detained by authorities, denied access to premises, or miss their flight.

Many biometric schemes effectively declare the individual to be guilty of something, and place the onus on the individual to

prosecute their innocence. That is repugnant to traditional concepts of justice. In addition, very few people understand how biometric systems work, and hence very few people are capable of dealing with such situations. Even for those individuals who do understand the technology, it's very difficult to find anyone administering the system who is capable of carrying on a sensible conversation about the errors involved.

6. Biometrics demand Strong Justification

Because biometrics technologies are so highly privacy-invasive, it is totally inappropriate for organisations to implement schemes without conducting very careful design, demonstrating the effectiveness of the scheme and the ineffectiveness of alternatives, performing privacy impact assessments (PIAs), conducting consultation with affected parties and their representatives and advocates, and preparing cost-benefit analyses that show conclusively that the benefits justify the costs and disbenefits to all parties involved, including and especially the people it is imposed upon.

All schemes have substantial downsides that impact on the people involved. Most potential biometric schemes fail the test, and should not be implemented. Those that have already been implemented should be subjected to critical assessment. This would result in the abandonment of many existing schemes, and the refinement of other schemes in order to ensure that they include appropriate safeguards.

7. Biometrics do not Stop Terrorism

Proponents of biometrics spread misinformation, suggesting that biometric schemes are necessary to combat terrorism. This is simply false (e.g. Schneier 2001, Ackerman 2003, Clarke 2003). Terrorists are defined by the acts that they perform, not by their biometric. Virtually no terrorist act, ever, anywhere, would have been prevented had a biometrics scheme been in operation.

8. Biometrics grant Excessive Power to Corporations and States

Biometrics lays the foundation for corporations and the State to extend their power over individuals. People are cowed by the knowledge that their actions are monitored and recorded. That substantially reduces their capacity to exercise the rights and freedoms that they are supposed to have.

Organisations are in a position to deny access to services, premises and transport to people whose identity they are unable to authenticate, or who they (rightly or wrongly) deem to be a particular person whom they have (justifiably or otherwise) blacklisted. Widespread application of biometrics could see these powers extended to something so far only seen in sci-fi novels and films – outright identity denial.

9. A Highly Intrusive Error-Prone Technology requires Tight Regulation

The protections that are needed against the ravages of biometrics include:

- legal frameworks
- public justification for the measure
- the obligation to perform a PIA
- the obligation to conduct consultations with affected individuals and their representatives and advocates
- mechanisms to ensure the outcomes of the PIA are reflected in the scheme
- features built into technologies and products
- features designed into manual processes
- laws regulating biometric technologies
- laws regulating the practices of all organisations
- enforcement mechanisms
- sanctions for breaches
- enforcement actions

10. Biometrics are Subject to Almost No Regulation

There is an almost complete absence of such protections. There are virtually no statutory protections in place.

A Biometrics Privacy Code has been published, and accepted by the Privacy Commissioner. The Code was produced by the so-called 'Biometrics 'Institute'. But that organisation is merely an industry association, and one that grossly compromises accepted principles by including both sellers and buyers inside a single lobby-group. And the purpose of the 'Institute' in publishing its Code was to forestall formal regulation. The public interest has been relegated to the role of an onlooker.

That Code has been almost completely ignored by technology providers and user organisations, and has had no impact at all on industry practices. Self-regulation in this, as in so many other areas, has been an abject failure. Yet if organisations had complied with even that weak and ineffectual Code, some of the gross excesses that companies and government agencies seek to impose would have been prevented.

APF thanks its site-sponsor: Hosted by GoWeb®

This web-site is periodically mirrored by
the Australian National Library's Pandora Archive
and by the Wayback Machine since March 2000

Biometrics in the Workplace

15 October 2011

Background

During the last few years, increasing numbers of employers have announced that they intend imposing biometric schemes on their employees, usually for the purposes of 'clocking on and off in the workplace'. Some have even gone ahead, ignoring the concerns of employees, unions, advocates and regulators.

Many employees are complacent about the idea. Buy many others feel considerable misgivings, some perceive themselves to be being treated with contempt, and some have serious concerns. However, particularly during periods of relatively high unemployment, many employees are hesitant to even question their employer's intentions, let alone oppose them.

Parliaments have abjectly failed to protect employees. There is very little law to support them when they seek ways to avoid having their bodies measured.

The APF has had a Policy Statement in relation to Biometrics for some years, which calls for a moratorium on all new biometrics schemes, and strong, statutory protections.

This document provides a brief statement of the Privacy Foundation's policy in relation to biometrics in the workplace. The links in the text below are to the relevant parts of the APF's general Policy Statement.

APF POLICY re BIOMETRICS in the WORKPLACE

Biometrics technology is highly privacy-intrusive.

Biometrics are highly error-prone and unreliable.

Biometrics are highly insecure.

Biometrics assist identity fraud and identity theft.

Biometrics create serious risks, which employees are forced to bear.

Applications of biometrics therefore demand strong justification. They must not be imposed just because an employer is powerful enough to get away with it.

Even if the circumstances warrant the use of biometrics, there must be substantial safeguards, to mitigate the many harmful aspects.

It is essential that proponents of biometrics schemes in the workplace:

- conduct a privacy impact assessment (PIA)
- as part of that PIA, provide information, in advance, to the people affected by it, including:
  - a sufficiently detailed description of the particular biometric technology
  - a sufficiently detailed description of the way in which it proposes to use biometrics
  - the justification for doing so
- as part of that PIA, undertake consultations, in advance of the decision whether or not to proceed, with representatives of the various categories of people affected by it, including relevant unions and social welfare organisations, and civil liberties and privacy advocacy organisations

---

The Biometrics Industry Self-Regulation Attempts Are a Complete Failure

The Biometrics 'Institute' is an unhealthy alliance of both suppliers of biometric technologies and user organisations. It has a weak Privacy Code that was designed as a defensive manoeuvre, in the hope that it would forestall the imposition of genuine regulation. It has been adopted by almost none of the Institute's members. The APF has called on the Privacy Commissioner to de-register the weak and ineffective Code.

The Code "covers the acts and practices ... 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".

Yet almost all proposals to apply biometrics in employment have been in breach of even that weak Code's provisions:

1. – Biometrics should not be collected unless it is "necessary" for business functions. (It isn't).

10. – "Sensitive information about an individual" – which a person's biometrics clearly are – must not be collected unless there is consent (which must be informed and freely given – and it isn't), or it is "required by law" (which it isn't).

12 – "Enrolments in biometric systems shall be voluntary, unless required by law". (Employers must permit 'free and informed consent' or 'opt-in' to the schemes. If they make submission to the scheme a condition of employment, then they are in breach of the Code).

APF thanks its site-sponsor: Hosted by GoWeb®

This web-site is periodically mirrored by
the Australian National Library's Pandora Archive
and by the Wayback Machine since March 2000

Created: 6 October 2011 - Last Amended: 15 October 2011 by Roger Clarke - Site Last Verified: 11 January 2009
© Australian Privacy Foundation Inc., 1998-2015 - Mail to Webmaster