Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

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

6 October 2012

Mr M. Hand
Managing Director of Retail Distribution
ANZ

Dear Mr Hand

Re: Biometrics at ATMs

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A brief backgrounder is attached.

The APF notes the article in Fairfax Media of 5 October 2012 to the effect that your company is considering the use of biometrics for customer authentication at ATMs.

We draw your attention to the APF's Policy Statement on Biometrics, and to a submission to Privacy Commissioners in relation to the need for national action on this matter, submitted jointly by APF and the nation's civil liberties organisations. Copies are attached.

It is widely recognised that all initiatives that have potentially negative implications for privacy need to be subject to a Privacy Impact Assessment (PIA) at an early stage in their development.

Would you please advise whether a PIA has been undertaken.

If so, would you please advise which advocacy organisations were involved, and how we can get a copy of the resulting PIA report?

If not, we submit that it is imperative that a PIA be undertaken, including consultation with consumer and privacy advocacy organisations.

We look forward to your reponse.

Thank you for your consideration.

Yours sincerely

Roger Clarke
Chair, for the Board of the Australian Privacy Foundation
(02) 6288 1472 Chair@privacy.org.au

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby and Elizabeth Evatt, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

•	Policies	http://www.privacy.org.au/Papers/
•	Resources	http://www.privacy.org.au/Resources/
•	Media	http://www.privacy.org.au/Media/
•	Current Board Members	http://www.privacy.org.au/About/Contacts.html
•	Patron and Advisory Panel	http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

•	The Australia Card (1985-87)	http://www.privacy.org.au/About/Formation.html
•	Credit Reporting (1988-90)	http://www.privacy.org.au/Campaigns/CreditRpting/
•	The Access Card (2006-07)	http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
•	The Media (2007-)	http://www.privacy.org.au/Campaigns/Media/

Australian
Privacy
Foundation

APF Policy Statement

POLICY Media Resources Campaigns | About Us What Can I Do? Big Brother Contact Us

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.

Created: 17 March 2008 - Last Amended: 15 October 2011 by Roger Clarke - Site Last Verified: 11 January 2009

New South Wales
Council for
Civil Liberties

Queensland Council
for Civil Liberties

Australian
Privacy Foundation

19 October 2011

Mr T. Pilgrim, Australian Privacy Commissioner

Dear Mr Pilgrim

Re: Biometrics

As you're aware, there's a current surge of activity by technology companies, trying to sell biometrics products to organisations of all kinds.

APF has published policy statements as follows:

- on Biometrics generally (Apr 2008, rev. Oct 2011), at: http://www.privacy.org.au/Papers/Biometrics.html
- on Biometrics in the Workplace (Oct 2011), at: http://www.privacy.org.au/Papers/Biometrics-Wkplace.html
- on Identity Scanning by Registered Clubs (Sep 2008), at: http://www.privacy.org.au/Papers/ClubIDScans.html

We believe that it's vital for the nation's Privacy Commissioners to publish clear and authoritative guidance on these matters that is designed to significantly influence organisational practices.

The personal data aspects of biometric schemes fall within your formal powers. We appreciate, however, that, in relation to aspects that threaten privacy of the physical person and privacy of personal behaviour, you may need to express your documents using somewhat different language.

Nonetheless, we submit that you are able to express positive statements about:

- the many seriously privacy-invasive aspects of biometrics
- the necessity of strong justification for the use of biometrics
- the likely breach of privacy laws if justification is not demonstrated
- the necessity of measures to mitigate negative privacy impacts the strong advisability of conducting privacy impact assessments of proposed new applications of biometrics, and of publishing the PIA report in time to influence decisions about the proposal
- the need for effective consultation processes with affected individuals and their representatives and advocates

We would appreciate your advice as to whether and when you will publish such guidance.

Thank you for your consideration.

Yours sincerely

Cameron Murphy, Chair NSW Council for Civil Liberties
Spencer Zifcak, Chair Liberty Victoria
Michael Cope, Chair Queensland Council for Civil Liberties
Dr Kristine Klugman, Chair Civil Liberties Australia
Dr Roger Clarke, Chair Australian Privacy Foundation