Australian
Privacy
Foundation

G.P.O. Box 1196
Sydney NSW 2001

enquiries@privacy.org.au

http://www.privacy.org.au

19 October 2007

Ms Judy Spence
Minister for Police and Corrective Services
PO Box 15195
City East QLD 4002

police@ministerial.qld.gov.au

Dear Ms Spence

Re: Biometrics of Visitors to Queensland Correctional Centres

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

I refer to the demands that visitors to correctional centres submit to biometric scanning, as at:
http://www.correctiveservices.qld.gov.au/About_Us/The_Department/Biometric_identification/index.shtml
http://www.correctiveservices.qld.gov.au/About_Us/The_Department/Biometric_identification/Biometric%20Factsheet%20Aug07.pdf

Biometrics are highly privacy-invasive, and the APF is extremely concerned about these measures. It seriously questions the need for them, and the scheme's design and procedures. The intensity of the issue is all the greater because of the use of private contractors to run some centres.

I attach an outline of the APF's concerns.

The APF formally requests that you suspend the scheme pending a comprehensive privacy impact assessment.

Yours sincerely

Roger Clarke
Chair, Australian Privacy Foundation, for the Board
(02) 6288 6916 chair@privacy.org.au

Attachment: Outline of Concerns

Biometrics are Extraordinarily Privacy-Invasive

Biometrics collection goes far beyond mere data issues. Biometrics involve physical impositions, and the extraction of something that is intrinsic to the individual. Moreover, biometrics are essentially unchangeable, and capture of them, and retention of templates, enables people to falsely represent themselves as someone else.

The assertion that "The system cannot convert the template back into a fingerprint image" may be technically true, but is grossly misleading. It has been shown many times that such templates can be easily used to generate an equivalent print that will pass the test. Every visitor is therefore subject to masquerade by anyone who gains access to the template. Because the data is stored centrally, the vulnerabilities extend far beyond the individual centres.

For these many reasons, the following are essential:

- all uses of biometrics need to be very specifically justified
- the justifications need to be subject to independent and public review
- the design of the system needs to ensure the minimum intrusivess and risk
- a comprehensive protection regime needs to be established in parallel with the scheme

The Need for Clear and Compelling Justification

The justifications provided on the web-site are so vague as to be completely meaningless: "improved access control" and "enhance the security of Queensland's high security correctional centres". What is the real, and specific, purpose of the scheme? If it is really an efficiency measure, is it appropriate to subject visitors to intrusive and demeaning procedures, and to risky capture and retention of data for such purposes? If it is actually intended as a means of clandestine capture of personal data for further purposes, what authority of law exists, and what protections?

The list of locations in which it is implemented or being implemented is stated to be already up to 7 centres, of the total of only 8+2 centres in existence. Are 7/10 really "high security" centres?

The collection of <u>any</u> form of identification information requires justification. The need for wand-searches and man-traps is clear. But on what basis is there any need to require the identity of a person seeking to visit a prisoner? On what bases are people precluded from making visits to prisoners in correctional centres? What actions have been taken on the basis of personal data collected in this way that would not have been feasible without that data?

If the scheme is primarily about the efficiency of second and subsequent accesses, then in respect of people who make a single visit to a corrective centre the scheme is wasteful for all concerned. What provisions are made for casual visitors who are unlikely to visit again?

Given that the scheme has already been implemented in some corrective centres, what evidence has been gathered that demonstrates that the scheme is effective in a security sense, e.g. how many extra people have been denied access to centres, and how many prosecutions have been commenced that would otherwise not have been possible?

The Expectation of Privacy Impact Assessment (PIA)

Your government expects privacy impact assessment (PIA) to be performed in relation to all significantly privacy-invasive initiatives. Has one been performed? What information was published to enable analysis to be performed? What organisations were consulted? Where was the PIA report published?

Is the Government a member of the Biometrics Institute? Is the design, and are the procedures, compliant with the Institute's Code? Are the privately-run correctional centres required to be members and to comply with the Code?

Accessibility, Equity and Discrimination Aspects

A significant number of people, as much as 5% of the population in the case of fingerprints, are physiologically unable to provide reliable biometric measurements. It is crucial, as a matter of public policy, that such people not be discriminated against.

Such 'outliers' may be detected at enrolment time, or the problem may already be known to the person concerned; but many people's inability to authenticate will only become apparent when they become a 'false-negative' on their second and subsequent visits. What procedures have been instituted to deal with these problems? What training has been provided to staff at the centres to deal with these circumstances in appropriate ways?

Recording of the appearance of the human body, including not only fingerprints but also the face, and interference with the integrity of the body more generally, give rise to serious concerns among people with various ethnic, cultural, religious and philosophical backgrounds. What provisions have been made for conscientious objection to biometric measurement? What training has been provided to staff at the centres to deal with these circumstances in appropriate ways?

Protections for Sensitive Personal Data

The template is very sensitive data, because it can be used as a means to generate an 'artefact', i.e. something that enables another person to pass authentication tests as though they were that person. (Note that date of birth is not a secret. 2 minutes' research found that the Minister's is 19 May 1957).

Even if justification can be shown for identity being needed, the data that is collected creates serious privacy concerns. Address is sensitive information for a proportion of the population, and the breadth of data required is close to that which is needed to perform identity theft.

The data that is collected is not subject to privacy protections at anywhere near the level of the OECD norms that have applied in the civilised world since 1980. The Corrective Services Act s.341 protection is limited to disclosure, which is only 1 of about a dozen aspects covered by conventional data protection laws.

No mention is made of State Government Standard No. 42. Is the agency exempt, or is this data not subject to the Standard? (Unfortunately, it is in any case a mere unenforceable code, and it is unclear whether it is respected even by the agencies that are subject to it).

The scheme appears to be already implemented in one of the private sector centres (Borallon). What protections apply in such circumstances? What measures are in place to inspect, enforce, and apply sanctions for breaches?

Some Queensland government agencies, and some practices within agencies, are exempt from the unenforceable 'Government Standard'. This is particularly the case with law enforcement agencies. Agencies of the Commonwealth, and of other State and Territory governments, may demand or request access to the data. After all, visitors are by definition in some sense 'associates' of criminals, and therefore of interest to law enforcement agencies. What protects the personal data, including the template, against acquisition by other agencies?

If no provisions are made for casual visitors, outliers and conscientious objectors, why should the public not suspect that the scheme's real purpose is to generate a database of people who associate with criminals, available for use for purposes unrelated to visits to correctional centres?

Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues which 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.

When necessary, the APF conducts campaigns 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 a participant in Privacy International, the world-wide privacy protection network.

Where possible, the APF cooperates with and supports official agencies. It is entirely independent of agencies set up to administer privacy legislation, however, and regrettably often it finds it necessary to be critical of those agencies.

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

The following pages provide access to information about the APF:

- papers and submissions http://www.privacy.org.au/Papers/
- resources http://www.privacy.org.au/Resources/
- media http://www.privacy.org.au/Media/
- Board-members http://www.privacy.org.au/About/Contacts.html

Examples of campaigns that it has been necessary to conduct are:

- the Australia Card (1985-87)
  http://www.privacy.org.au/About/Formation.html
- the Consumer Credit Extensions to the Privacy Act (1988-89)
- Data Matching Programs (1991-93)
- the Integrated Public Number Database (IPND) (1997-99)
- the Internet whois database (2001)
- the APEC Privacy Framework (2003-04)
- the Medicare Smart Card (2004-06)
  http://www.privacy.org.au/Campaigns/ID_cards/MedicareSmartcard.html
- the Human Services Card (2005-06)
  http://www.privacy.org.au/Campaigns/ID_cards/HSCard.html
- the Australia Card Mark II (2005-06)
  http://www.privacy.org.au/Campaigns/ID_cards/NatIDScheme.html
- the Human Services 'Access Card' (2006-)
  http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html