TECHNOLOGICAL ASSAULT on visitors to prisons

James Godfrey

With touches of sci-fi technology the application of biometric identification to visitors to NSW prisons raises issues of cost, effectiveness and privacy.

At present, there are three conventional forms of identification: something you have, like a card; something you know, like a password or PIN; and finally something which you are, like your fingerprints, voice, image, or any other identity trait.[1] One of the problems of taking fingerprints and photographs is that these acts are associated with criminality — indeed any intrusive identification system will be seen as such.

'Biometrics are technologies which automatically verify one's identity based on physiological characteristics;'[2] biometric identification includes retina scans, voice recognition and hand geometry. It has been used at such diverse places as a Los Angeles sperm bank, San Francisco International Airport and a childcare centre at the Lotus Corporation in the USA.[3] One company (Biometric Tracking LLC) even requires people to enrol their fingerprints in a database in order to gain access to its web site.

The exponential growth in biometrics identification system (BIS) is under way; indeed the 'global market for biometric technologies is estimated to be in excess of $50 billion'.[4] In order to expand its business, the biometrics industry has begun to target the 'captive markets' (the armed forces and prisons). Such involvement opens up the path for operation in the 'closed systems' (immigration control, access control, voter registration and state benefits registration). Once this has taken place, the way will be cleared for biometrics to intrude into the 'open markets' (employment, banking, health etc.).[5]

Biometric identification in NSW prisons

This article focuses on the imposition of fingerprint scanning of visitors to maximum security prisons in New South Wales. On 8 August 1996, the Department of Corrective Services (DCS) implemented a BIS at Maitland prison. By the end of 1996, it had been introduced to prisons at Goulburn and Lithgow, as well as the Remand Centre, the Special Purpose Centre and the Reception and Induction Centre at Long Bay. On 4 July 1997, the largest application of the system to date in NSW began at the new $85 million Metropolitan Reception and Remand Centre (MRRC) at Silverwater — the largest prison in Oceania, currently holding nearly 900 prisoners. Although the BIS was originally intended only to be used for those visiting maximum security prisons, there is a major problem in relation to remand centres. The MRRC is deemed maximum security and yet many of the people detained there are merely awaiting trial for minor offences.

The procedure

The BIS currently operating consists of two actions of registration. First, a video image is taken of the visitor's face. This image is then linked to a key code, which identifies the person's fingerprints. For the fingerprinting exercise, DCS utilises equipment that takes a photo of two thumbs, or a thumb and a forefinger, then identifies the eight best features by two-dimensional topography. It then converts these fea-

James Godfrey is a law student at the University of New South Wales.

tures, by applying a unique algorithm, into a digital number (key code) and destroys the actual photo.

When a visitor goes to a prison, they must place their thumb and/or forefinger onto a pad, which is linked to the database. The DCS official should then be able to see the image of that person on the computer monitor. Although apparently only to be used for adult males, there have been some instances when children as young as four have been scanned.

Although DCS has claimed the information obtained will be secure, the inherent dangers that could arise from authorised access and networking, let alone unauthorised access and disclosure are potentially enormous, particularly as the image is stored on a clipboard — even if, only momentarily. The DCS's system is produced by Fingerprint Technologies, which also has supplied a major part of the Offender Management System (OMS) that aids in the control of prisoners. David Owens from DCS insisted that the two systems are totally separate.[6] However, even the Commissioner, Leo Kelliher, admits it could be technically feasible for this system to share information with other systems such as those operated by the police.[7]

The DCS has installed a package of hardware and software fully capable of capturing and recording fingerprint scans (used for inmates), capturing individual personal data comparable to the current OMS, and fully networking with other internal and external databases. The potential also exists for a fingerprint image to be recreated from an individual key code. No mention is made of the Department's backup or archives system, which must necessarily exist to prevent visitor data being lost in a system crash. If such data is backed up via a network connection to another hard or portable drive on the premises or elsewhere, it will be extremely vulnerable. If data is backed up in a way that it can be copied or stored onto other media, it can then be transported to other systems and databases. Thus, the current BIS is inherently insecure, and the potential breaches of a person's privacy are alarming.

Privacy laws

> Developments in technology and international communications technologies are rendering our privacy laws hopelessly out of date ... A recent European Community directive will have the effect of excluding Australian entities from European Community data flows unless our privacy laws are substantially improved by mid-1998.[8]

Despite ongoing debate, NSW does not, as yet, have its own privacy legislation. Consequently, NSW prisons are not subject to any privacy laws; as the *Privacy Act 1988* (Cth) only applies to the Commonwealth public sector. The debate around BIS may give some impetus to a much needed campaign for State privacy legislation, which can reflect today's concerns about privacy protection. Such legislation would obviously need to take account of the massive growth in technology outsourcing, privatisation and corporatisation that has taken place in recent years.

Perhaps an act similar to the *Privacy Act 1993* (NZ) would be appropriate. It stipulates that personal information shall not be collected by any agency unless the collection of the information is necessary for that purpose (pple 1(b)). Furthermore, it prohibits any agency from collecting personal information by means which intrude to an unreasonable extent on the personal affairs of the individual concerned (pple 4(b)(ii)). There are also safeguards requiring an agency holding personal information to ensure the information is protected against loss and that it is not inappropriately accessed, modified or disclosed (pples 5(a)(i) and (ii)). It also prohibits an agency from keeping information for longer than is required (pple 9). In addition, any privacy legislation must contain some penalties for breaching the law. Given the paucity of privacy protection afforded to people in NSW, the need for extensive regulation of the BIS is obvious.

Regulating the BIS

The Minister for Corrective Services may make regulations prescribing 'visits to ... correctional centres ... and admission generally to correctional centres' (s.50(g) *Correctional Centres Act 1952* (NSW) CCA) and also 'visits to and correspondence by and with inmates' (s.50(i) (CCA). Whether the Minister must make regulations about certain matters and the exact extent of his power is currently being examined by Justice Action, a community action group.

One year after introducing the BIS into some prisons in NSW, DCS eventually issued a draft copy of a Regulation, which purported to authorise the system and provide safeguards. On 14 August 1997, a draft *Prisons (General) Amendment (Biometric Identification System) Regulation 1997* was sent to the Criminal Justice Coalition (CJC) for it to comment on by 29 August. This time limit was extended for a further two weeks to allow for 'community consultation'. The CJC decided not to officially comment on the proposed Regulation until the NSW Privacy Committee had met, discussed and responded in detail. Months later, the CJC is still waiting for the Committee to respond in some public way about the scheme. While the Privacy Committee has kept its thoughts on the matter private, a revised Regulation was tabled in State Parliament. Late last year, some Green and Independent Members of the Upper House tried to disallow the Regulations—however this was defeated by the Government and the Liberal opposition.

Problems and objections to the use of biometric identification

Whereas every inmate of a prison is to be photographed, to have the impression of their fingers and palms taken, and to have such details of their personal description as may be prescribed recorded (s.19 CCA), no such requirement exists for visitors.

Security

The supposed impetus for the introduction of the BIS was that it would improve prison security — specifically following the escape of the late George Savvas in 1996. If prison officers are unable to detect a prisoner changing clothes and donning a wig during a visit, then surely there is little chance they can ensure they press the right buttons or check that the face in front of them matches the face on their monitors. A further issue relating to security is that the BIS is being used arbitrarily. Prison officers, legal visitors and many other people are gaining access into prisons without having to submit themselves to fingerprint scanning, inevitably reducing the supposed security the BIS provides.

Indigenous issues

The Aboriginal Legal Services have reported some Indigenous women are making the difficult choice not to visit family members rather than allow themselves to be scanned for fear of having this information shared with other government

departments. More importantly, their traditional beliefs necessitate they leave no image or record behind when they die and they are unwilling to take the chance they have involuntarily done so when scanned. Statements are currently being obtained from various Indigenous peoples to enable their beliefs to be respected and taken into account.

Consent

A major objection to this scheme — in contrast to that in operation in Queensland — is that it places visitors to prisons in a position where they cannot give informed consent to having images of their fingerprints and their face taken, which might reduce the waiting time during visits. In NSW, rather than sacrifice their visit most people will submit to this non-consensual process.

Physical problems

There are problems which will arise with people who have fine-skinned fingers,[9] recent burns, wounds and, of course, with amputees. DCS staff have even told some women that lanolin and ingredients of washing-up liquid can prevent the scanner from working properly.

Security of information

Due to genuinely held fears that the BIS may be interfaced to police, social security or immigration computers many visitors may avoid prisons. Indeed, on 3 September at the MRRC, some visitors preferred to forfeit their visit and chat with the writer and others while other members of their family went inside. The procedure led John Akister from the Council of Civil Liberties to accuse DCS of 'attempting to assert powers that even the police did not have ... imposing measures which were regarded as measures only applied to criminals'.[10]

Delays

Since the introduction of the BIS, there have been many reported incidents of extensive delays in the processing of visitors. An example occurred on 19 July 1997, when all of the visitors to Long Bay were turned away because of problems with the biometrics identification equipment. Other instances were acknowledged at the newly opened MRRC by one of the officers who revealed that visitors had had to wait on occasions for up to three and a half hours to get into the Centre and up to two hours to get out. The prison authorities solution? All visits must now be booked in advance and are limited to 30 per two-hour period.

Alternatives to biometric identification of visitors

The system DCS introduced into the prisons serves no purpose other than to further criminalise and harass friends and families of inmates. Even though very few prisoners actually escape through the visiting area of NSW prisons (only three in the last five years), the small number of cases could be eradicated by the introduction of any one of these different mechanisms:

- If biometric fingerprint identification must be used, then surely to meet security needs, only prisoners' identification needs to be taken. Every person exiting the prison could be scanned and any print matching a prisoner's would cause an alarm to sound. No permanent record would be maintained and there would be minimal privacy concerns for visitors.
- Alternatively, each visitor could be stamped with some kind of unique (perhaps ultra-violet) stamp, which could be changed each day. In turn, this could be read on the way out.
- Another option would be to implement a procedure whereby each prisoner was taken after a visit, to a designated area and checked before their visitor is allowed to leave the centre.

Conclusion

Clearly the imposition of the biometrics identification system currently in use throughout the maximum security prisons of NSW cannot be justified. It is intrusive, expensive and ineffective. It serves no purpose other than to further intimidate visitors and ultimately may damage the essential links that prisoners have with the outside world. It must go and the multitude of problems that similar systems may cause to individuals in our society must be examined in detail.

References

1. Davies, S., 'Touching Big Brother — How Biometric Technology will Fuse Flesh and Medicine', (1994) 7(4) *Information Technology and People* 2.
2. *Business Wire*, 27 August 1997, New York.
3. Miller, B., 'Vital Signs of Identity', *IEEE Spectrum*, Institute of Electrical and Electronic Engineers, New York, February 1994, p.25.
4. Core Ventures Inc. newsletter, 26 August 1997, New York, on OTC bulletin board, citing a research report conducted in England in 1994.
5. 'Biometrics Briefing', *Privacy International*, Washington DC, 1997.
6. Unofficial minutes taken by T. Anderson of Council for Civil Liberties of a DCS Biometrics Meeting, 1 May, 1997.
7. See minutes of meeting of 21 May 1997 between DCS and ten members of the CJC.
8. The Liberal/National Coalition Law and Justice Statement issued immediately before the last Federal election, cited in Australian Privacy Foundation letter to Prime Minister John Howard, 28 March 1997.
9. Florida Times Union website 19 July 1997 which detailed the story of an Indian woman who has finally been exempted from supplying fingerprints to the US Immigration Department after 11 unsuccessful attempts to obtain a readable set of prints from her hands.
10. Unofficial minutes, above, ref. 6.