



25 May 2005



Senator Nick Bolkus
Chair
Senate Legal and Constitutional Committee
Department of the Senate
CANBERRA ACT 2600

GPO Box 5057
Melbourne Victoria 3001
Australia
DX 210643 Melbourne

Level 11
10-16 Queen Street
Melbourne Victoria 3000
Australia

Telephone +61 3 8619 8719
Local Call 1300 666 444
Facsimile +61 3 8619 8700
Local Fax 1300 666 445

www.privacy.vic.gov.au
enquiries@privacy.vic.gov.au

Attn: Ms Sophie Power
Principal Research Officer
Committee Secretariat

Dear Senator Bolkus,

Inquiry into the Privacy Act 1988 (Cth)

I refer to Ms Sophie Power's email of 5 May 2005 seeking my views on a question I agreed to take on notice at the public hearing I attended on 22 April 2005. Senator Natasha Stott Despoja asked for further comments on the protection of genetic information, and on how well-equipped the law is to deal not just with emerging technologies, but with microchips.

Protection of genetic information

I refer the Committee to previous submissions I have made in this area:

- Submission (and Supplemental Submission) to the Victorian Parliament's Law Reform Commission on its Inquiry into Forensic Sampling and DNA Databases, July and September 2002;
- Submission to the Forensic Procedures Review Committee on its Review of Part 1D of the *Crimes Act 1914 (Cth)*, September 2002;
- Submission to the Australian Law Reform Commission and Australian Health Ethics Committee on its joint inquiry into the Protection of Human Genetic Information, December 2002; and
- Submission to the Victorian Law Reform Commission on its Issues Paper into Workplace Privacy (including genetic testing in the workplace), April 2003.

As you will see from these submissions (all of which are available on www.privacy.vic.gov.au), there are a number of gaps in the law affecting genetic privacy, including:

- the lack of clarity over the ability of privacy laws to provide protection and redress for those whose genetic privacy is at risk;
- the need to consider the implications of genetic knowledge not only in predicting health conditions and predispositions, but also as capable of indicating physical traits and behavioural predispositions;
- recognition that genetic knowledge can be used for non-health purposes, notably for establishing identity, paternity and kinship;
- the potential for mass DNA testing to coerce individuals not suspected of a crime to giving up their DNA without sufficient protections under law to minimise the risk of coercion, or to ensure prompt destruction of their DNA when no longer required;
- the lack of regulation over non-consensual collection of DNA for paternity testing;
- the uncertainty over ownership of DNA, over whether anyone can hold property in someone else's DNA, and whether the donor can assert control over who may access their body tissue and the information that may be derived from analysing their body tissue;
- the vulnerability of DNA samples collected and stored for therapeutic uses (eg newborn screening) to be used for other, unrelated uses, without the knowledge or consent of the individuals whose body tissue was taken (or of their parent or guardian);
- the ease with which genetic samples are discarded and capable of being collected and submitted for testing without the knowledge or consent of the individuals affected, and without the authority of a court;
- the use of covert collection of DNA by police outside of the forensic procedures laws, and therefore outside of the safeguards regulating notice, use, matching, retention and destruction; and
- setting the boundaries in relation to when a person's blood relatives have a "right to know" the outcome of genetic test results, and when an individual has a "right not to know" their genetic indicators.

Microchips which can be implanted in human beings

Although Radio Frequency Identification (RFID) was initially used primarily for tracking objects (such as individual items of foodstuff, clothing and books), it is gradually being used to track people (such as children) by embedding RFID chips in clothing or cards. The use of RFID raises significant privacy issues around how it is used, when its use is justifiable, what other information is made accessible through the use of the device, and what safeguards apply to minimise the risk of misuse and provide redress. I refer the Committee to the work of international data protection and privacy commissioners:

- International Conference of Data Protection & Privacy Commissioners, *Resolution on Radio-Frequency Identification*, 20 November 2003, <http://www.privacyconference2003.org/resolutions/res5.DOC>;
- Article 29 Data Protection Working Party (set up under the EU Data Protection Directive 95/46/EC), *Working document on data protection issues related to RFID technology*, WP 105, 19 January 2005.

I also refer the Committee to recent overseas proposals in this area:

- US Federal Trade Commission, *Radio Frequency Identification: Applications and Implications for Consumers*, workshop, 21 June 2004, staff report and workshop presentations available at <http://www.ftc.gov/bcp/workshops/rfid/index.htm>;
- EPCGlobal's *Guidelines on EPC for Consumer Products*, [Electronic Product Code is an emerging system that uses RFID], 2005 (referred to in the US FTC's RFID report above), http://www.epcglobalinc.org/public_policy/public_policy_guidelines.html;
- EPIC's *Guidelines on Commercial Use of RFID Technology*, 9 July 2004, http://www.epic.org/privacy/rfid/sb682_33005.html;
- Californian legislative proposal to ban the use of RFID in State identity documents: *Identity Information Protection Bill 2005*, SB689, http://info.sen.ca.gov/cgi-bin/postquery?bill_number=sb_682&sess=CUR&house=B&site=sen.

The Committee's Terms of Reference specifically refers to the chip recently approved by the US Food and Drug Administration. This chip is described by the manufacturer, Verichip (<http://www.4verichip.com/verichip.htm>), as follows:

The VeriChip miniaturized Radio Frequency Identification [sic] (RFID) Device is the core of all VeriChip applications. About the size of a grain of rice, each VeriChip contains a unique verification number, which can be used to access a subscriber-supplied database providing personal related information. And unlike conventional forms of identification, VeriChip cannot be lost, stolen, misplaced or counterfeited.

Once implanted just under the skin, via a quick, painless outpatient procedure (much like getting a shot), the VeriChip can be scanned when necessary with a proprietary VeriChip scanner. A small amount of Radio Frequency Energy passes from the scanner energizing the dormant VeriChip, which then emits a radio frequency signal transmitting the individuals unique verification (VeriChipID) number.

In the USA, the chip is used to identify patients and enable access to their health information (<http://www.fda.gov/cdrh/ode/guidance/1541.pdf>). It is likely that RFID chips will find other applications, where tracking identifiable individuals is sought. According to Verichip, the technology is "being actively developed for a variety of security, defense, homeland security and secure-access applications, such as authorized access control to government and private sector facilities, research laboratories, and sensitive transportation resources" (<http://www.4verichip.com/verichipfuture.htm>).

The company manufacturing Verichip (Applied Digital) has also recently completed research into "an implantable prototype unit that combines global-positioning satellite technology with a cell phone, identification chip and a battery. The unit employs GPS as a locator, then uses the cell phone to transmit a signal. The device, which measures 1.25 x 0.5 inch, could be surgically inserted beneath a user's collarbone" (http://www.4verichip.com/nws_07262004.htm).

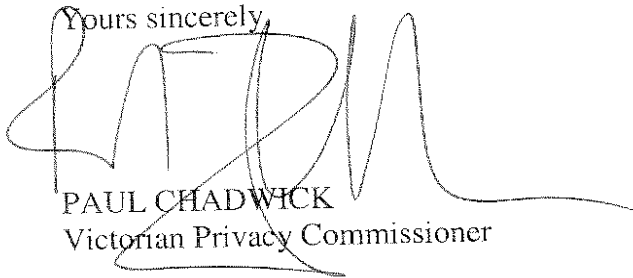
Implanting the device under the skin raises additional privacy concerns that need to be debated. Although the use of electronic monitoring has recently been authorised under law in respect of serious sex offenders released from custody, the legislation (*Serious Sex Offenders Monitoring Act 2005 (Vic)*) is silent as to whether a tracking device can be implanted under the ex-offender's skin. (The more common way to track offenders or others released conditionally from detention is through devices such as bracelets on wrists or ankles that are secure against being removed or disabled.) Any such interference with bodily integrity, if ever contemplated in extraordinary circumstances, should only be done under clear authority of law or by

voluntary and informed consent, and with appropriate safeguards to protect the health, privacy and dignity of the individual to be tracked, and those with whom he or she lives and associates.

If the Committee has any further queries, please do not hesitate to contact me.

I wish to acknowledge the work of Michelle Fisher, OVPC Manager, Policy, in the preparation of many of the OVPC materials referred to in this letter, and in collation of the other references.

Yours sincerely,

A handwritten signature in black ink, appearing to be 'P. Chadwick', written over the typed name and title.

PAUL CHADWICK
Victorian Privacy Commissioner