Office of the
Victorian Privacy
Commissioner

Office of the Victorian Privacy Commissioner

(Privacy Victoria)

Submission to

the Commonwealth Senate

Legal and Constitutional Committee

on its

Inquiry into the Privacy Act 1988 (Cth)

March 2005

TABLE OF CONTENTS

1 Introduction

1. Privacy – subtle, abstract, instinctive privacy – is easily over-valued in a brochure, luncheon speech or a doorstep interview (where it matters least), and just as easily under-valued in crafting a statute, or implementing an administrative scheme or finalising a contract (where it matters most).

2. The Committee's present task, as it examines in 2005 the *Privacy Act* borne of the Australia Card debate of the late 1980s, is twofold –

    a. How is Australia to value privacy commensurate with privacy's status as a basic human right that is under stress in a technology-fuelled Information Age when security fears are high?

    b. How is Australia to value privacy sufficiently when privacy necessarily is balanced with other public interests in running public administration (increasingly, e-government), and the economy (increasingly, e-commerce)?

3. A hard-headed answer to the first question will help guard against self-delusion, complacency or a false sense of security.

4. Agile yet diligent efforts to respond to the second question will help to ensure that Australia reaps the benefits of the information and communications technologies (ICT) while also minimising their risks, of which a principal risk is the loss of individual privacy in multiple governmental and commercial situations.

5. Doubtless, many other submitters will illustrate for the Committee the many situations in which privacy can be at risk. These situations, and attempts to avert or to conciliate them when they lead to breaches, are the daily bread of a Privacy Commissioner's office. Term of Reference a. ii. lists four categories in which the situations will increasingly arise: smart cards, biometrics, genetics and microchip implants.

6. But this submission will not analyse the many situations or try to suggest detailed responses to them. The risks are manifold, but they vary with the information involved, the technologies employed and the countervailing interests/benefits. The submission does not omit them because they do not matter. They do, because they render practical what is abstract (and we all tend to under-value the abstract). They make human a concept that most people take for granted, until it is gone.

7. A Privacy Commissioner's office seems uniquely placed to submit, for the Committee's attention, a 'satellite view' of the contemporary scene, leavened by practical experience. We are specialists. You Senators are generalists. But all of us, and, according to consistent research results, the overwhelming majority of the public, care about our own privacy and the privacy of those we love.

2 Why the significance of privacy law is growing

8. The *Privacy Act 1988* is in need of strengthening. It is of greater urgency now than it was in 1988 that the privacy of Australians be protected under a robust, flexible national scheme, administered independently of the Executive and widely understood by the public.

9. Briefly, the reasons include –

Technological developments

10. ICT will not abate – nor should it - and the need to balance its benefits and its privacy risks will not abate.

Putting international standards into domestic law

11. Australia is a signatory to the leading human rights instruments that incorporate a right to privacy. It is easy to miss the connections between privacy and the practical availability of other basic rights. Privacy is an instrumental freedom, in the sense that it plays a role in the enjoyment of freedom of expression, freedom of association and freedom of belief.

12. Remote, with a relatively small population and a First World economy, Australia has a special need to foster its links into the major economic groupings. The adequacy of Australia's privacy protection scheme has been doubted by the EU. Australia was active in the preparation of privacy standards for APEC, adopted last year.

13. Australia's scheme would be more effective if workplace privacy were to be more comprehensively addressed.

The effects of the events of 11 September 2001

14. The focus on the threat of terrorism since 11 September 2001 has put a focus on the balance between liberty and security. In various pieces of legislation in the Commonwealth and State Parliaments, a general trend to reduce liberty in favour of increased security can be discerned. Terrorism and major crime have tended to be conflated, and police powers have generally been increased. Put broadly, the domestic police forces have become more like intelligence agencies and the intelligence agencies have been given more police-like roles.

15. These developments can be charted through several Senate inquiries and the work of various State-based entities.

16. Other jurisdictions have reported a trend of greater sharing of personal information between the private sector and public sector security and law enforcement.

17. It is not possible to estimate how long the tilt towards security and away from liberty will last. But it is a fact that those who have been further empowered, by the proper authorities, will generally be able to intrude into privacy to a greater degree than in the past.

18. It will therefore be necessary to remain vigilant, so that the powers are exercised according to the proper safeguards. Judicial oversight and parliamentary review are

two safeguards. Others are the existence of national enforceable privacy standards and of an independent Privacy Commissioner's Office, where staff with the requisite specialist expertise can assist the accountability process. OFPC can provide explanations about proper standards and international comparisons. The public can complain and bring to the attention of the appropriate decision-makers, through the Commissioner, any problems that may arise from the recent re-balancing of liberty and security.

19. Some new measures included sunset clauses. When parliaments come to reconsider whether the measures should be extended, they will need adequate data on which to make the assessment.

3 Committee's Terms Of Reference

Overall effectiveness

International comparisons

20. Privacy Commissioners and Data Protection Commissioners in most developed economies of the world face roughly the same issues. The technologies are global, the commercial pressures to gather and use personal information are similar, and most governments have increased security and police powers at the expense of privacy since 11 September 2001.

21. The Committee will find a wealth of data relevant to any strengthening of the Privacy Act 1988 in the resources listed later in this submission.

22. Generally speaking, although relatively small and low-powered in the scheme of things, the commissioners' offices are useful barometers of the likely weather patterns for the Information Age. OFPC is no different, and that is another reason to ensure it is given the powers, independence and resources adequate to its task.

23. In the Information Age, data protection has an economic imperative, as much as a civil liberties or human rights rationale. The New Zealand Privacy Commissioner, Marie Shroff, has recently laid stress on this important but poorly understood dimension of privacy laws. Victoria's *Information Privacy Act* was conceived in the 1990s by the then Treasurer, and developed by the section of the bureaucracy devoted to growing the information economy. While it incorporates a basic human right into Victorian law, it also has an expressly economic development motive. Essentially, it has been widely recognised that unless you build confidence and trust in the new technologies by reassuring people about their privacy, you will not reap the benefits of your investment in those technologies via e-government and e-commerce. The Committee will find the background and the rationale further explained in various OVPC documents including its Website Guidelines and Public Registers Guidelines, available at www.privacy.vic.gov.au

24. This hybrid motivation – human rights/economic driver - was less prominent in 1988, when the *Privacy Act 1988* was enacted. It would improve the Act if it were better articulated, without sacrificing the human rights aspect of the rationale, which has a deep historical pedigree (borne out of the 1948 Declaration) as well as continuing

relevance. Technologies are often transient, but privacy endures as a deep human instinct, an aspect of freedom and a human right.

Capacity to respond to emerging technologies

25. It is not possible to analyse these broad topics in this submission. Instead, some pithy basics about each, from a privacy perspective –

Smart cards

26. The dumber the better, unless they include safeguards for privacy, accessibility to the data they hold for the data-subject, an option of anonymity where that is feasible (eg public transport smartcards, which offer terrific benefits if done well). A key question is: who controls the back office and is accountable for the subsequent use, disclosure, accuracy and security of the data gathered and distributed via smartcards?

Biometrics

27. Many types are being developed and aggressively marketed, especially to governments, which can be ideal customers because they buy in large quantities and have weak shareholder accountability. Different biometric devices have varying reliability and levels of intrusiveness as identity management tools. It is essential to conduct a Privacy Impact Assessment before biometrics are introduced. This should be mandated if any mass application of biometrics are considered in future and the public will be unable to exercise an informed, voluntary choice about whether to participate.

Remaining items in the Terms of Reference

28. Other matters may be relevantly covered in a supplementary submission or at a hearing, if the Committee requests it.

4 Conclusion

29. By sketching the scene, in Australia and internationally, and commenting on several prominent features of it, this Office hopes it has persuaded the Committee that answering the two questions posed in the Introduction means that the Committee should give consideration to the following matters.

    a. whether a right to privacy ought be enshrined in the Constitution or a Human Rights Act, potentially encompassing rights to "Respect for private and family life" and to the "Protection of personal data" (as is done in Articles 7 and 8 of the *Charter of Fundamental Rights of the European Union*).

    b. strengthening of the *Privacy Act 1988 (Cth)*, in light of contemporary and foreseeable developments, in relation to data protection, including -

        i. harmonising the IPPs that have governed the federal public sector since 1989 with the NPPs that apply to much of the private sector, with particular regard for trends such as outsourcing, privatisation and public-private partnerships;

ii. taking account of cross-border harmonisation of security and law enforcement powers affecting privacy by improving commensurately cross-border accountability of security and law enforcement entities;

iii. compelling greater transparency in the collection and handling of personal information by the public and private sectors, including greater notice about data sharing arrangements (as California does in relation to business sharing information with marketers under the "Shine the Light" Law) and about security breaches to enable those persons affected to take immediate action to mitigate any harm they may suffer, including identity theft (as California has also done by enacting legislation applying to both private sector and government agencies);

c. strengthening of the *Privacy Act 1988 (Cth)*, in light of contemporary and foreseeable developments internationally, in relation to genetic privacy, including –

i. considering the recommendations of the Australian Law reform Commission in its Report, *Essentially Yours: Protection of Human Genetic Information*;

ii. having regard to UNESCO's *International Declaration on Human Genetic Data*, passed unanimously and by acclamation by the General Assembly in October 2003;

iii. taking account of any rights of the "biological group" to know, and of the individual not to know, the results of genetic tests, as raised by the Article 29 Data Protection Working Party (established under the EU Data Protection Directive) in their *Working Document on Genetic Data*, published in March 2004;

d. strengthening of the *Privacy Act 1988 (Cth)*, in light of contemporary and foreseeable developments, to ensure comprehensive protection in respect of existing and emerging technologies including:

i. considering whether existing national and state interception and surveillance laws provide adequate protection for individuals as they engage in activities in public and private places, as they communicate by print or electronic means, and as they leave "data trails" as they travel throughout the community;

ii. ensuring that privacy protection is in place to regulate particularly intrusive technological devices, such as RFID-enabled microchips implanted in a person's body;

e. ensuring powers, independence, resources and accountability for the Office of the Federal Privacy Commissioner is commensurate with: the significance of the right to privacy as a basic human right; and the complexity of OFPC's tasks in the contemporary and foreseeable governmental, commercial, social and technological context;

f. recognising expressly the natural tensions arising for a statutory office such as Privacy Commissioner when it is part of the Executive yet must regulate the Executive in relation to privacy. (Like freedom of information law, privacy law recalibrates legally enforceable rights and obligations over information, and that means it recalibrates power, at least to some extent. Knowledge being power, this makes for tensions.)

g. establishing a funding and accountability model for OFPC that comprises at least:

    i. independent assessment of the resources needed in the forthcoming year by OFPC;

    ii. direct appropriation from Parliament; and

    iii. the capacity for the Privacy Commissioner to directly table reports in Parliament.

PAUL CHADWICK

Victorian Privacy Commissioner

4 March 2005

Selected references

GENETICS

Office of the Victorian Privacy Commissioner, *Submission to the Forensic Procedures Review Committee on its Review of Part 1D of the Crimes Act 1914 (Cth)*, September 2002, http://www.privacy.vic.gov.au Publications > Reports and Papers > Submissions.

Australia, Forensic Procedures Review Committee (Tom Sherman, Chair), *Report of the Independent Review of Part 1D of the Crimes Act 1914 – Forensic Procedures*, March 2003, http://www.ag.gov.au/part1d.

Australian Law Reform Commission & Australian Health Ethics Committee report, *Essentially Yours: The Protection of Human Genetic Information in Australia*, March 2003 (tabled in Parliament in May 2003), http://www.austlii.edu.au/au/other/alrc/publications/reports/96/.

See especially:

- in relation to privacy laws:
  - chapters 7 – amending and harmonising information and health privacy laws to provide legally enforceable privacy standards for genetic information and genetic samples;
  - chapter 8 – providing individuals with a right of access to their own sample and, where necessary to lessen or prevent a serious threat to life, to that of their first-degree genetic relatives;
- in relation to non-consensual genetic testing:
  - chapter 12 – enacting a new criminal offence prohibiting the submitting a genetic sample for testing, or testing a genetic sample, without consent or other lawful authority;
- in relation to genetic research:
  - chapter 15 – reviewing the *National Statement on Ethical Conduct in Research Involving Humans* to ensure that its provisions for waiver of consent and reporting of decisions is consistent with privacy laws;encouraging best practice in human genetic research, including developing consent forms that allow for graduated consent options, disclosure of actual or anticipated commercial arrangements, ownership or property interests in samples or genetic information, and withdrawal of consent by participants;
  - chapter 17 – strengthening review by Human Research Ethics Committee, including greater transparency, oversight and accountability in reviwing human genetic research;
- in relation to parentage testing of a child's sample:
  - chapter 35 – prohibiting parentage testing unless done under a court order or with the consent of a child who is aged 12 years and of sufficient maturity (or otherwise with the consent of all persons with parental responsibility for the child);
- in relation to law enforcement access to, and use of, genetic samples:
  - chapter 18 – developing rules for disclosure of newborn screening cards and other samples for law enforcement purposes only with consent or pursuant to a court order;
  - chapter 40 – harmonisation of Australian forensic procedures laws with respect to the collection, use, storage, destruction and index matching of forensic material and the DNA profiles created from such material;
  - chapter 41 – amending the Crimes Act to deal with informal collection of genetic samples by providing that law enforcement officers may, with the exception of crime scene samples, only collected genetic samples from the individual concerned pursuant to a forensic samples order, or to a stored sample with the individual's consent or pursuant to a court order.

United Kingdom, Human Genetics Commission and UK National Screening Committee, Joint Working Group on Profiling Babies at Birth, http://www.hgc.gov.uk/Client/Content.asp?ContentId=159.

> The Joint Working Group was established as a result of a request by the UK Government in its White Paper on Genetics (details below) to "conduct an initial analysis of the ethical, social, scientific, economic, and practical considerations of genetic profiling at birth" (see paragraphs 3.36-3.38). According to the HGC's website, the Working Group plans to report by March 2005.

United Kingdom, Department of Health, *Our Inheritance, Our Future: Realising the Potential of Genetics in the NHS*, white paper presented to Parliament by the Secretary of State for Health, June 2003, http://www.dh.gov.uk/assetRoot/04/01/92/39/04019239.pdf.

United Kingdom, Nuffield Council on Bioethics, *Genetics and Human Behaviour: The Ethical Context*, October 2002, http://www.nuffieldbioethics.org/go/ourwork/behaviouralgenetics/publication_311.html.

United Nations Educational, Scientific and Cultural Organization (UNESCO), *International Declaration on Human Genetic Data*, adopted unanimously and by acclamation on 16 October 2003 by the 32nd session of the General Conference of UNESCO, http://portal.unesco.org/shs/en/ev.php@URL_ID=2444&URL_DO=DO_TOPIC&URL_SECTION=201.html.

BIOMETRICS

United States, Department of Health and Human Services, Food and Drug Administration, *Class II Special Controls Guidance Document: Implantable Radiofrequency Transponder System for Patient Identification and Health Information*, Guidance for Industry and FDA Staff, December 2004, http://www.fda.gov/cdrh/ode/guidance/1541.pdf.

VeriChip, http://www.4verichip.com/verichip.htm. The overview on the site says:

> The VeriChip miniaturized Radio Frequency Identifcation (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.

Barnaby J. Feder & Tom Zeller Jr., "Identity Badge Worn Under Skin Approved for Use in Health Care", *New York Times*, 14 October 2004, http://www.nytimes.com/2004/10/14/technology/14implant.html.

> This NY Times article discusses the FDA's approved use of VeriChip and mentions the Mexico Attorney-General's announcement re: usage of RFID implants.

Biometrics Institute Ltd, *Draft Privacy Code*, submitted to the Office of the Federal Privacy Commissioner, May 2004, http://www.biometricsinstitute.org/bi/codeofconduct.htm.

PRIVACY AND THE MEDIA

Paul Chadwick (Victorian Privacy Commissioner), *Privacy and Media - subtle compatibility - five categories of fame*, presented to the 26th International Conference on Privacy and Personal Data Protection, Wroclaw, Poland, 15 September 2004, http://www.privacy.vic.gov.au > Publications > Speeches.

SURVEILLANCE & EMERGING TECHNOLOGIES

European Commission, Joint Research Centre, Institute for Prospective Technological Studies, *Security and Privacy for the Citizen in the Post-September 11 Digital Age: A Prospective Overview*, 2003, http://www.jrc.es/home/publications/publication.cfm?pub=1118.

DATA MATCHING

Data-matching Program (Assistance and Tax) Act 1990 (Cth), http://www.comlaw.gov.au.

Australia, Office of the Federal Privacy Commissioner, *Data Matching Program (Assistance and Tax) Guidelines (Annotated version),* September 1991, http://www.privacy.gov.au/act/datamatching/.

Australia, Office of the Federal Privacy Commissioner, *The use of data matching in Commonwealth administration – Guidelines,* February 1998, http://www.privacy.gov.au/act/datamatching/.

INTERNATIONAL COMPARISONS OF PRIVACY LAWS

Elecronic Privacy Informatino Center (EPIC) and Privacy International, *Privacy & Human Rights 2004: An International Survey of Privacy Laws and Developments*, 7th annual privacy and human rights survey, 2004, http://www.privacyinternational.org/phr.

> Note esp the comments on international trends re: resources, in the Overview section, under "Oversight and Privacy and Data Protection Commissioners":
>
> A major problem with many agencies around the world is a lack of resources to adequately conduct oversight and enforcement. Many are burdened with licensing systems, which use much of their resources. Others have large backlogs of complaints or are unable to conduct significant number of investigations. Many that started out with adequate funding find their budgets cut a few years later.
>
> Independence is also a problem. In many countries, the agency is under the control of the political arm of the government or part of the Ministry of Justice and lacks the power or will to advance privacy or criticize privacy invasive proposals. In Japan and Thailand, the oversight agency is under the control of the Prime Minister's Office. In Thailand, the director was transferred in 2000 after conflicts with the Prime Minister's Office. In 2001, Slovenia amended its Data Protection Act in order to establish an independent supervisory authority and thereby ensure compliance with the Data Protection Directive. This was previously the responsibility of the Ministry of Justice.
>
> Finally, in some countries that do not have a separate office, the role of investigating and enforcing the laws is done by a human rights ombudsman or by a parliamentary official.

International Conferences on Privacy and Personal Data Protection:

- 18th conference, Ottawa, Canada, September 1996, http://www.privcom.gc.ca/speech/archive/02_05_a_960918_e.asp
- 19th conference, Brussels, Belgium, September 1997, http://web.archive.org/web/20001216031700/www.privacy.fgov.be/conference/papers.html
- 20th conference, Santiago de Compostela, Spain, September 1998,
- 21st conference, Hong Kong, September 1999, http://www.pco.org.hk/english/infocentre/conference.html

- 22nd conference, Venice, Italy, September 2000, http://www2.garanteprivacy.it/garante/prewiew/0,1724,1619,00.html?sezione=116&LANG=1
- 23rd conference, Paris, France, September 2001, http://web.archive.org/web/20011005023732/www.cnil.fr/conference2001/eng/welcome.html
- 24th conference, September 2002,
- 25th conference, Sydney, Australia, September 2003, http://www.privacyconference2003.org/
- 26th conference, Wroclaw, Poland, September 2004, http://26konferencja.giodo.gov.pl/
- 27th conference, Montreux, Switzerland, September 2005, http://www.privacyconference2005.org/

European Commission, Article 29 Data Protection Working Party, established by Article 29 of *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, http://europa.eu.int/comm/internal_market/privacy/index_en.htm.

Asia-Pacific Economic Cooperation (APEC), *APEC Privacy Framework*, 2004/AMM/014rev 1, endorsed by the 16th APEC Ministerial Meeting, Santiago, Chile, 17-18 November 2004, http://www.apec.org/apec/news___media/2004_media_releases/201104_apecminsendorseprivacyfrmwk.html.

OTHER OVPC PUBLICATIONS COMMENTING ON PRIVACY IMPACT OF LEGISLATIVE AND LAW REFORM PROPOSALS

Relevant OVPC submissions, most of which are available at http://www.privacy.vic.gov.au > Publications > Reports and Papers > Submissions:

Genetics

Forensic sampling and DNA databases, Submission to the Victorian Parliament Law Reform Committee, July 2002

Forensic Sampling and DNA Databases (supplemental), Supplemental Submission to the Victorian Parliament Law Reform Committee, September 2002.

Protection of Human Genetic Information, Submission to the Australian Law Reform Commission and Australian Health Ethics Committee joint inquiry, December 2002

Terrorism & law enforcement powers

Terrorism (Community Protection) Bill 2003, Submission to the Victorian Parliament's Scrutiny of Acts and Regulations Committee, 19 March 2003.

Cross-Border Investigative Powers for Law Enforcement, Submission to the Standing Committee of Attorneys-General and the Australasian Police Ministers Council Joint Working Group on National Investigation Powers, 5 June 2003
Major Crime Legislation (Office of Police Integrity) Bill 2004 & Major Crime (Special Investigations Monitor) Bill 2004, Submission to the Victorian Parliament's Scrutiny of Acts

and Regulations Committee, September 2004 (available at http://www.parliament.vic.gov.au/sarc/2004alerts/Appendix_4_alert_7.htm).

Major Crime (Investigative Powers) Bill 2004, Submission to the Victorian Parliament's Scrutiny of Acts and Regulations Committee, October 2004.

Surveillance and interception

Surveillance Devices Bill 2004, Submission to the Commonwealth Parliament's Senate Legal and Constitutional Committee, 23 April 2004
Telecommunications (Interception) Amendment Bill 2003, Submission to the Senate Legal & Constitutional Committee, 12 March 2004; and

Telecommunications (Interception) Amendment (Stored Communications) Bill 2004, Submission to the Senate Legal & Constitutional Committee, 28 June 2004.

Location information

The future use of location information to enhance the handling of emergency mobile phone calls, Submission to the Australian Communications Authority, 7 May 2004, (Text has been corrected for printing errors only.)

Spatial Information in Victoria, Submission to the Review Panel on a Regulatory and Administrative Framework for Survey and Spatial Information in Victoria, December 2002.

Spatial Information Privacy Best Practice Guideline, Submission to ANZLIC, the Spatial Information Council, on its draft Privacy Best Practice Guideline, December 2003.

Victorian Spatial Information Strategy, Submission to Land Victoria on the draft Spatial Information Strategy 2003-2006, 3 April 2003.

Employee records & workplace privacy

Information privacy and employee Records, Submission to the Australian Government, April 2004

Workplace Privacy, Submission to the Victorian Law Reform Commission, 11 April 2003

Public registers

Privacy and publicly available personal information, Comments to the Federal Privacy Commissioner, , September 2002 (not available online)

Direct marketing

Direct Marketing Model Code of Practice, Submission to the Ministerial Council on Consumer Affairs, October 2002.

The spam problem and how it can be countered, Submission to the National Office for the Information Economy, October 2002