ORWELL OR ALL WELL?
The rise of surveillance culture

ROBERT CHALMERS

Big brother is watching you[1]

It was an inevitable reaction to specific acts of terrorism, as well as the broader evolution of crime and technology, that governments in Australia and elsewhere would seek to increase and update their legal ability to surveil their citizens and others, in order to track, respond to and possibly pre-empt criminal acts. There is nothing new about state surveillance, but there have clearly been considerable advances in technology that alter the potential balance and boundaries of private and public information and activities. These new technologies may be used to either enhance or — more commonly — intrude on privacy and civil liberties (to the extent those are actually recognised by our systems of law in the first place).

Other commentators have already observed that many of the recent legislative interventions, though on the surface initiated by and directed against terrorist attacks, have a much broader functionality. For example, the Patriot legislation in the US[2] (the very title of which reads like Orwellian *newspeak*)[3] contains a number of provisions that extend general law enforcement powers, some of which may be used to counter terrorism, but which are by no means so limited in terms of their legal reach or actual use.

In Australia over recent years there have been a number of actual or proposed reforms directed at extending and updating intelligence agency and law enforcement powers of surveillance, both at the federal and at the state level. These include reforms to telecommunications interception, the regulation of use of surveillance devices, and the practical roll-out of expanded closed-circuit camera systems. There are also efforts to implement systems and laws dealing with the problem of authentication of identity, especially in an online environment and in the context of the growing problem of 'identity theft'. It is in this area of identity in particular that the boundaries between public and private surveillance start to blur. For most people, private sector surveillance of behaviour for commercial purposes is probably a more fundamental, pervasive and perhaps offensive issue than government surveillance. In this private sector area there are relatively few effective checks and balances, either regulatory or technical. How should the law and the general public respond to all these issues? Is there cause for concern?

Recent Australian reforms

Easy access to email

At the federal level, one of the most recent changes to surveillance powers has been the exemption of email from some of the access controls under the interception regime established by the *Telecommunications (Interception) Act 1979* (Cth).[4] Obviously, when that regime was first established the possibility of email was not contemplated. However, due to the broad framing of the legislation, there was a concern that accessing emails stored on a computer network technically fell within the ambit of those controls. Security and law enforcement interests did not want to be burdened with compliance with the warrant systems designed for telephone intercepts *per se* and successfully lobbied for exemption of email from the coverage of the Act. This move was subject to much criticism, as now arguably any legal power of compulsion can be used to justify access to stored communications, with no warrant requirement.[5] Proponents of the change justified the move on the basis of an analogy between mail and email, but opponents rejected this on the basis that email is a hybrid form of near instantaneous communication. Note that communication by 'voice over Internet protocol' was expressly not exempted from the standard controls, and indeed in terms of user perception it is basically a phone call, even if mediated via different computer networks. Similarly, other communications stored on a highly temporary basis (eg momentary buffering in a router) potentially remain within the ambit of the pre-existing laws, though it is not clear whether this would include so called 'instant messaging' services allowing computer users to key 'live' or 'always on' email-like messages to each other.

These provisions were reviewed by Anthony Blunn, whose report has now been delivered to Parliament.[6] As an interim response the federal government has introduced the Telecommunications (Interception) Amendment (Stored Communications and Other Measures) Bill 2005 (Cth) to extend the 2004 approach for a further six months beyond the original 14 December 2005 sunset date, and to allow proper consideration of the Blunn Report. However, the Attorney General was pleased that the report seemed to show the *Telecommunications (Interception) Act 1979* (Cth) was 'remarkably robust in an age of revolutionary technological change'.[7] This *doublethink* 'spin' is somewhat hard to reconcile with many of the key findings of the Blunn Report:

REFERENCES

1. George Orwell, *Nineteen Eighty-Four* (first published 1949, 1954 ed) 5.

2. *Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism* (USA PATRIOT ACT) *Act of 2001* Pub L No 107–56, 115 Stat 272, see especially Title II 'Enhanced Surveillance Procedures'.

3. See also Eric Wolff, 'What's In a Name? Plenty, Lawmakers Have Realized', *The New York Sun* (16 April 2004) <http://www.igorinternational.com/press/new-york-sun.html> at 1 February 2005.

4. As amended by the *Telecommunications (Interception) Amendment (Stored Communications) Act 2004* (Cth).

5. See, eg, Australian Privacy Foundation, *Re: Review of the Regulation of Access to Communications under the Telecommunications (Interception) Act 1979* (20 May 2005) [36]–[42] <http://www.privacy.org.au/Papers/SubmTelecomInterceptI050520.pdf> at 9 November 2005.

6. Anthony S Blunn AO, *Report of the Review of the Regulation of Access to Communications* (August 2005) <http://www.ag.gov.au/blunnreview> at 20 September 2005 (Blunn Report).

7. Philip Ruddock MP, 'Telecommunications Interception Changes To Help Agencies To Fight Corruption' (Press Release, 14 September 2005) <http://www.ag.gov.au/agd/WWW/MinisterRuddockHome.nsf/Page/Media_Releases> at 20 September 2005.

At the federal level, one of the most recent changes to surveillance powers has been the exemption of email from some of the access controls under the ... Telecommunications (Interception) Act 1979 (Cth).

- the language and detail of the *Telecommunications (Interception) Act 1979* are increasingly limiting in terms of accommodating new and emerging technologies, in terms of industry development and in terms of responding to the needs of security and law enforcement agencies ...
- the present distribution of functions relating to accessing telecommunications data for security and law enforcement purposes between Parts 13, 14 and 15 of the *Telecommunications Act 1997* and the *Telecommunications (Interception) Act 1979* is complicated, confusing and dysfunctional;
- as presently structured, the *Telecommunications (Interception) Act 1979* is not an appropriate vehicle for accessing other than real time communications;
- the provisions of the *Telecommunications Act 1997* governing access to stored communications are inadequate and inappropriate ...[8]

Most notably, the key recommendation of the Blunn Report was that 'the protection of privacy should continue to be a fundamental consideration in, and the starting point for, any legislation providing access to telecommunications for security and law enforcement purposes'.[9] Other changes to be introduced by the 2005 Bill include allowing various state-based anti-corruption commissions to use intercepted material to investigate corrupt conduct. However, it should be noted that the Victorian Office of Police Integrity will not be permitted to use such material 'until the Victorian Government addresses concerns about appropriate oversight'.[10]

Private sector co-operation with law enforcement

It is also important to remember the ways in which private sector carriage and Internet service providers are co-opted into implementation of, and co-operation with, elements of the State's surveillance infrastructure, quite apart from the specific powers under the *Telecommunications (Interception) Act 1979* (Cth). For example, the Australian Communications Industry Forum has published a code on assistance to law enforcement agencies, elaborating a scheme of practice based on Part 14 of the *Telecommunications Act 1997* (Cth). The ACIF Code requires service providers to give security and law enforcement agencies 'reasonably necessary' help for the purposes of enforcing the criminal law, as well as laws imposing pecuniary penalties, protecting the public revenue and safeguarding national security.[11] Common types of assistance called for include 'subscriber details, call charge records, reverse call records ... call tracing ... suspension of carriage services ... telecommunications services, products and technical advice for use by an Agency in connection with an investigation'.[12] Requests for access may be made direct to organisations, either with or without certificates authorising the access. While access to communications content and personal information is more tightly controlled, it is available in some circumstances.

Recent and proposed changes to regulation of the use of surveillance devices

Another recent change to surveillance laws at the federal level is the *Surveillance Devices Act 2004* (Cth), which introduced a new scheme to pull together, update and extend various scattered provisions relating to the use of surveillance devices by federal law enforcement or security agencies. It arose out of a summit on terrorism and multijurisdictional crime held on 5 April 2002, but relates to policing activities generally and is not targeted specifically at terrorism. It seeks to enable effective law enforcement use of all manner of surveillance devices, including enhanced imaging equipment, tracking systems, cameras, microphones and software ('data surveillance devices'). The Attorney General justified the legislation by claiming that 'surveillance device laws available to Commonwealth law enforcement are not up the job of 21st century policing'.[13] The Act is meant to enable police to 'match and better' criminal and terrorist groups, while containing a range of checks and balances, authorisation procedures, and warrant requirements. Some of the newer features introduced include provisions relating to installation of authorised 'spyware' (in stark contrast to the approach proposed for unauthorised private sector spyware, discussed further below). The Act also permits more general use of surveillance devices for any Commonwealth or federally related state offence that carries at least a three-year maximum penalty (which of course a great number do), rather than the current limited prescribed range of offences. This 'floor' on offence seriousness is meant to ensure that 'an appropriate balance is struck between the public interest that law enforcement investigate serious offences and the privacy interests of individual Australians'.[14]

On 8 September 2005, the Prime Minister announced a series of further controls to combat terror, pre-empting the 27 September 2005 Council of Australian Governments (COAG) meeting. The Prime Minister's proposals included reforms to the Australian Secret Intelligence Organisation's special powers warrant. This will be altered to clarify the definition of 'electronic

8. Blunn, above n 6, 5–6.

9. Ibid 5.

10. Ruddock, above n 7.

11. Australian Communications Industry Forum (ACIF), *Industry Code — Provision of Assistance to National Security, Enforcement and Government Agencies* (June 2001) <http://www.acma.gov.au/acmainterwr/telcomm/industry_codes/codes/c537.pdf> at 20 September 2005.

12. Ibid, Code Rule 2.1.3.

13. Commonwealth, *Parliamentary Debates*, House of Representatives, 24 March 2004, 27010 (Philip Ruddock, Attorney General).

14. Ibid 27011.

equipment'; allow entry onto premises; extend the validity of search warrants for computer access (from 28 days to three months) and the validity of mail and delivery service warrants (from 90 days to six months); and permit removal and retention of material for an indefinite period ('such time as is reasonable "for the purposes of security"').[15] At the COAG meeting, the Commonwealth and States agreed on enhanced tracking (perhaps even 'pre-crime' electronic bracelets for people subject to control orders) and other extended law enforcement powers, subject to extended sunset provisions (10-year sunset clause, with a review after five years). In the lead up to this agreement, the Commonwealth Attorney General had opposed shorter sunset proposals, on the basis that 'if they are unusually short, what you are saying to the agencies who are involved is that rather than focus on your core responsibilities of protecting the Australian community, you should be preparing for a review'.[16] Legislation has now been introduced further to the COAG meeting, in the form of the Anti-Terrorism Bill (No 2) 2005 (Cth).

Even prior to the COAG meeting, state governments were also keen to be seen to be heavy on terror and crime and strong in protecting the public. Several state governments announced their own tough anti-terror measures, again criticised by many legal groups as being an unnecessary incursion on civil liberties.[17] In addition, there were announcements of additional closed-circuit TV monitoring and pictures in the popular press of prominent politicians and others sitting in the panoptic centres 'watching over us'. These images are potentially simultaneously comforting and intimidating, if not vaguely ridiculous: the full glare of the public media brought to bear on a supposedly 'secret' control room.[18]

Implications of enhanced surveillance powers

The enhancement of government surveillance powers raises a host of issues, including whether these extensions are: (a) justified by circumstances; (b) general in nature or targeted at specific types of activity; (c) technology neutral or technology specific and dependent; (d) of indefinite duration or subject to formal review and sunset; and (e) appropriate to their defined purpose or unnecessarily intrusive on other rights (eg privacy and civil liberty more generally). A further very significant issue is what checks and balances exist for the exercise of these powers, in terms of authorisation, implementation, reporting, oversight, complaint and review. Politically, it is yet to be seen how far the public is willing to tolerate the intrusive aspects of such controls in light of the 'benefits' (tangible and intangible) that they deliver.

In the present climate, with the rush to introduce further changes, there is a danger that systems will be designed without sufficient checks and balances up front. There is also the ever present danger of abuse of systems. We have seen this numerous times in the past, whether in relation to politically motivated 'McCarthyist' practices of the Cold War, abuse of information systems for private gain, or the examples of information being leaked from Victorian police information systems.[19] Consider also the claims that the Defence Signals Directorate abused telecommunications interception powers to illegally intercept civilian calls in the context of the *MV Tampa* crisis. While the Inspector General of Intelligence and Security concluded that allegations of abuse for political purposes were unfounded, he did find serious breaches of operational protocol and insisted on implementation of preventative measures, as well as apologies to individuals whose communications were inappropriately intercepted. He even identified some procedural changes to improve the operation of his own office to effectively perform its oversight and review function.[20]

The problem of identity and identification

Another important and interlinked issue is that of personal identification. The federal government has a range of initiatives underway in this area, from biometric passports, possible changes to the 'in person' 100 point identity check currently required by the *Financial Transaction Reports Act 1988* (Cth), and the more general issue of validation of identity for government-related transactions (whether social security, medical benefits related, or otherwise) through to apparently mundane matters such as the more secure new wedding certificate announced on 1 September 2005 by the Attorney General. In the health sector there are moves to establish unique patient identifiers to produce a more efficient health system, cutting down on unnecessary or inappropriate treatments and unintended drug interactions, and providing ready access to full medical history. However, this Health*Connect* initiative has been subject to many delays and there are still many fundamental issues to address around database design, privacy, security and access control measures, and liability.[21]

There is also considerable and warranted concern about 'identity theft' crimes, and law enforcement initiatives to attempt to deal with such problems. State governments have also been updating some identity-related measures, including driving licences (eg Queensland's 'smart card'), though in the face of privacy concerns there have been subsequent announcements to try to reassure the public that these measures are not about imposing some form of 'Australia Card' by stealth.[22] South Australia has introduced identity theft provisions into its criminal laws.[23] And as a result of the COAG meeting on 27 September 2005, Australian governments are working on other strategies to counter identity crime, on the basis that '[t]he preservation and protection of a person's identity is a key concern and right of all Australians'.[24]

In relation to the identity check required by the *Financial Transaction Reports Act 1988* (Cth), mentioned above, the federal government is now coming under considerable pressure from those elements (mostly

15. Prime Minister, 'Counter-Terrorism Laws Strengthened' (Press Release, 8 September 2005) <http://www.pm.gov.au/news/media_releases/media_Release1551.html> at 20 September 2005.

16. Sophie Morris, 'Ruddock opposed terror clause', *Australian Financial Review* (Sydney), 26 September 2005, 4.

17. See, eg, Law Council of Australia, 'Terrorism: The New Law and Order Auction?' (Press Release, 14 September 2005) <http://www.lawcouncil.asn.au/read/2005/2417440788.html> at 16 November 2005.

18. 'First pictures inside secret surveillance bunker 400 cameras watch you', *The Advertiser* (Adelaide), 14 September 2005, 5.

19. In relation to the last of these, see, eg, 'Officer faces punishment for LEAP leak', *theage.com.au*, 12 October 2005 <http://www.theage.com.au/news/national/officer-faces-punishment-for-leap-leak/2005/10/12/1128796574556.html > at 2 November 2005.

20. Inspector General Intelligence and Security, 'MV Tampa, August– September 2001 — Collection and Reporting of Intelligence Relating to Australians' (April 2002) <http://www.igis.gov.au/tampa_statement.cfm> at 20 September 2005.

21. Commonwealth of Australia, *Lessons Learned from the MediConnect Field Test and HealthConnect Trials* (April 2005) <http://www7.health.gov.au/healthconnect/pdf/lessons1-10.pdf > at 6 October 2005.

22. Simon Hayes, 'Licence not an ID card', *The Australian* (Sydney), 30 August 2005, 32.

23. *Criminal Law Consolidation Act 1935* (SA) ss 144A-F (in 'Pt 5A—Identity theft').

24. COAG Special Meeting on Counter-Terrorism, *Communiqué* (27 September 2005) <http://www.coag.gov.au/meetings/270905/index.htm#Identity> at 28 September 2005.

The Surveillance Devices Act 2004 (Cth) seeks to enable the effective use of all manner of law enforcement use of surveillance devices, including enhanced imaging equipment, tracking systems, cameras, microphones and software ...

foreign) of the financial services industry that do not have a significant branch presence in Australia, and hence would dearly love to have the local laws permit fully online applications for financial services (as is the case in some other jurisdictions). They are very keen to piggy-back on government-sanctioned identity checks if possible. This has not yet been approved in Australia and is reportedly being resisted strongly by other lobby groups and corporate banking interests, including the Commonwealth Bank, which believes the current requirement for a person to physically front up for an identity check is an essential element, given the limits of current online authentication methods.[25]

Future problems may also arise from other attempts to introduce new technologies to act as tokens of government-sanctioned identity. For example, radio frequency identification technology, as commentators have observed elsewhere, may be used by commercial information service providers or others to track individuals and their behaviours.[26]

Private surveillance — is there sufficient safeguard?

An issue which is probably of even more significance than that of government surveillance is the pervasive surveillance that most of us are subject to in our everyday activities (whether online, in a store, on the phone or elsewhere) from a multitude of often invisible 'little brothers': companies with a commercial interest in building and using profiles of our behaviours and identities, either for their own purposes or through on-sale or co-operation with other entities (often cross-border). While the gathering of this information may be lawful, or even 'consented to' contractually by a consumer (though often unknowingly), it also carries with it enhanced risks of privacy intrusion and identity theft if these corporate databases of personal information are compromised.[27]

There is some regulation in this area, including by the *Privacy Act 1988* (Cth), flawed as it is. The private sector elements of the Act were recently (internally) reviewed and found largely satisfactory, though further review was contemplated, and a possible need for change in some areas was flagged.[28] Despite this, many commentators would argue that the level of effective protection offered to individuals by the Act is woefully low, especially when the level of complaints and the paltry resourcing of the Office of the Federal Privacy Commissioner are taken into account.[29]

More recently, Senator Brian Greig (Australian Democrats, Western Australia) introduced the Spyware Bill 2005 (Cth), which is directed against so-called spy and ad ware tracking the behaviour and identifying information of unknowing computer users. However, there appear to be many potential gaps in this Bill, in terms of limitations in the definitions and major exceptions to the Bill's application (see especially sub s 5(2)). And there are obvious jurisdictional problems in attempting to curb such activities, especially in what is an increasingly online and cross-border trading environment. Therefore, isolated attempts to regulate such software might appear to be largely ineffective flag-waving exercises, even if appropriately targeted. There needs to be a much larger and harmonised international effort to reduce such problems.

And beyond the 'private commercial' sector, there is growing agitation around unwanted personal surveillance (especially mobile phone camera and hidden video surveillance) in the purely private sphere.[30] In New Zealand this concern led to the introduction of specific controls in the Crimes (Intimate Covert Filming) Amendment Bill 2005 (NZ). In Australia the posting of such images to websites is now the subject of an enquiry and a discussion paper issued by the Standing Committee of Attorneys General on 9 August 2005.[31]

On the upside, there is some debate around the positive effects of the use of surveillance technologies and communication tools such as the Internet to provide a broadly based private 'watch on the watchers' — so called *sous*veillance, although critiques of this sort of approach include the dangers of its co-option to the cause of surveillance.

Biometrics and other magic wands

Biometrics are often touted as the answer to identification problems, and the federal government is rushing to follow a US lead in biometric passports, to improve identification and stop entry of undesirable people at borders and to reduce passport fraud. More generally, biometrics have been promoted as providing secure solutions to problems of access control, whether in security, general government or private sector applications. However, as even many of the more reputable biometrics advocates will acknowledge, biometrics alone are not the answer. Indeed, without overarching and robust security architectures and sensible approaches to privacy issues, such systems have the potential to be hijacked just like any other identifier, but to perhaps devastating effect. While you

25. 'Online ID checks open door to foreign banks', *The Financial Review* (Sydney), 7 September 2005, 1.

26. See, eg, Bruce Schneier, 'Fatal Flaw Weakens RFID Passports', *Wired News* (3 November 2005) <http://www.wired.com/news/privacy/0,1848,69453,00.html> at 7 November 2005.

27. See, eg, ABC Television, 'Your Money and Your Life', *Four Corners* (15 August 2005) <http://www.abc.net.au/4corners/content/2005/s1435556.htm> at 20 September 2005.

28. Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (March 2005) <http://www.privacy.gov.au/act/review/index.html> at 20 September 2005.

29. See, eg, Australian Privacy Foundation, *Review of Privacy Act 1988 private sector provisions* (December 2004) [4] <http://www.privacy.org.au/Papers/index.html> at 16 November 2005.

30 See, eg, Garry Barker, 'I spy with my little mobile ...', *theage.com.au* (6 December 2003) <http://www.theage.com.au/articles/2003/12/05/1070351787829.html> at 14 November 2005; and Office of the Victorian Privacy Commissioner, 'Mobile Phones with Cameras', *Info Sheet* (28 August 2003) <http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/5E60D920487E4F34CA256D9000251656/$FILE/05.03Phonecam_MFcredit9pt.pdf> at 21 September 2005.

31. Standing Committee of Attorneys General, *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, Discussion Paper (August 2005) <http://www.ag.gov.au/agd/WWW/agdhome.nsf/0/86D0F0FBE6DE7B85CA25705700050C1F?OpenDocument> at 28 September 2005.

can be reissued with a new credit card, you cannot be so easily reissued with a new set of fingerprints, eyeballs or other features in the event of compromise of the biometric data.[32]

There is no perfect technical or regulatory wand (biometric or otherwise) that will fix our identification problems. Rather, a cluster of strategies needs to be adopted, while recognising fraud will continue indefinitely. Systems need to be designed to be privacy sensitive and to respond rapidly to compromise of their integrity, as well as include good design that lowers the chance of violations occurring in the first place.

Brothers in arms: public and private surveillance — how to respond?

The modern day *big brother* image has changed from that envisaged by Orwell. There is no longer a moustache — now the focus is on slightly quizzical but still omniscient and omnipotent bushy eyebrows. Our real 'big/little brother' issue is a combination of the usual human failings and insecurities: fear and greed. The public or state aspects, while being the most visible manifestations of power, are really only a small part of the overall picture in a society where the state is increasingly privatised. Indeed, our society has become acculturated to, and saturated with, surveillance. Often each individual aspect of increased surveillance — for example obvious video surveillance on public transport — has a benign aim. However, the growing pervasiveness of the surveillance we are now subject to, combined with the technical power to integrate (at least in theory if not so easily in practice) these different sources of surveillance conjures up nightmare visions of identity theft or annihilation (as popularised by Sandra Bullock in the 1995 Hollywood film *The Net*).

On the other (private sector) hand, the new commercialised version of *big brother* also has considerable state and even religious connotations, including absolute power, and the ability to protect or to cast the citizen out of the Garden of Eden. In keeping with modern style and the needs of home product suppliers, this 'garden' is now largely an internal built environment (with the possible exception of a few pot plants around the spa). Indeed, it is interesting to see, in programs such as the Ten Network's *Big Brother*, the private sector simultaneously preying on our voyeuristic tendencies while milking personal or demographic data (and revenue) from downloads, competitions and SMS. But whether in relation to commercial matters or public sector national security, there is the traditional implicit dichotomy of the 'included' and the 'excluded', where those with a (perhaps state) sanctioned and verified identity will have more ready access to benefits such as goods, services and citizenship (at the 'price' of enhanced susceptibility to tracking of their behaviour), but where those without such identity will struggle.[33]

Surveillance has become normalised in many ways, and people have built up a tolerance for it. But that tolerance is not inexhaustible. A kick back will undoubtedly occur at some point and on a broader scale, especially in the face of abuses, whether these are abuses in the public or private sectors. It is perhaps to an extent already visible in some of the controls on the abuse of workplace surveillance, such as the *Workplace Surveillance Act 2005* (NSW) — a path Victoria seems set to expand on in the wake of the recent Victorian Law Reform Commission report into such issues[34] — and the growing complaints in relation to abuse of personal information in the marketing space. Consider also the recent controversy over Telstra supposedly authorising snooping and the compilation of secret dossiers on its staff's personal activities.[35] On an alternative reading (eg to an in-house corporate lawyer) this situation might display nothing more than a fairly unremarkable fusion of an employer's ability to self-protect against fraudulent behaviour, with a privacy policy on the handling of such information. But the public discussion and perception of this, albeit arguably gingered up by media promotion of a 'visceral' issue, displays a much greater level of anxiety about what is really going on. And it is that perception that is important in terms of maintaining or breaking overall public confidence that privacy (whatever that nebulous concept entails) is being adequately observed.

It is critical that those involved in designing, regulating or implementing systems of surveillance be particularly mindful of their negative potential, and be more respectful of underlying human rights issues. Without such careful attention we will confront an increased risk of these tools being used, in subtle or unsubtle ways, both visible and invisible, to oppress rather than benefit the greater public good.

Even more importantly, the broader public must get involved in an informed debate about these issues and take responsibility for protecting themselves. Alternatively, each of us can just sit back in our easy chairs, watching our telescreens uncritically with gin (and tonic?) in hand and follow Winston's example:

> He was back in the Ministry of Love, with everything forgiven, his soul as white as snow. He was in the public dock, confessing everything, implicating everybody. He was walking down the white-tiled corridor, with the feeling of walking in sunlight, and an armed guard at his back. The long-hoped-for bullet was entering his brain ... He gazed up at the enormous face ... Two gin-scented tears trickled down the sides of his nose. But it was all right, everything was all right, the struggle was finished. He had won the victory over himself. He loved Big Brother.[36]

ROBERT CHALMERS teaches law at the University of Adelaide.

32. Although there are some potential ways of addressing this, see, eg, 'Distortion to fool ID thieves', *The Australian* (Sydney), IT Broadsheet, 13 September 2005, 4.

33. For discussion of the possible exclusion of classes of people by the introduction of biometric identification see, eg, Duncan Graham Rowe, 'Privacy and prejudice: whose ID is it anyway?', *New Scientist*, 17 September 2005 (No 2517), 20–21.

34. Victorian Law Reform Commission, *Workplace Privacy*, Final Report (October 2005) <http://www.lawreform.vic.gov.au/CA256902000FE154/Lookup/Privacy/$file/Privacy%20Final%20Report.pdf> at 6 October 2005. [See also the Brief in this edition on p 286. Ed]

35. 'Telstra keeps secret staff dossiers', *The Australian* (Sydney), 31 August 2005, 5.

36. Orwell, above n 1, 239–40.