Government Surveillance in Australia

CONTENTS

Government Surveillance in Australia

Nigel Waters

Nigel Waters is Principal of Pacific Privacy Consulting. He was Deputy Australian Federal Privacy Commissioner from 1989-1997, and before that Assistant UK Data Protection Registrar. He is Principal Researcher on the Interpreting Privacy Principles project at the Cyberspace Law and Policy Centre, at UNSW. He holds Masters degrees from the Universities of Cambridge and Pennsylvania and from the University of Technology, Sydney.

This paper is based on work commissioned by Professor James Rule of the State University of New York, Stony Brook in June 2006, for his forthcoming book 'Privacy under Pressure'.

Some introductory comments

Major terrorist incidents (both the US incidents in 9/11/01 (more particularly for Australia the Bali bombings in October 02 and October 05, and the London bombings of July 2005) gave additional impetus to an existing trend towards a surveillance society. There have been no radical new departures but instead an acceleration in the type and amount of surveillance and the ease and speed with which it has been authorised.

Increases in surveillance have been effected not only by increasing the powers of various government agencies to access information, but also, more fundamentally, by requiring a range of organisations in both the public and private sector to collect and store more information about customers and transactions. These requirements, effected through a range of disparate legislation and regulations, is not always primarily or even incidentally intended to give the authorities greater access – often it is in pursuit of other public interests such as improved consumer protection or corporate governance, or health and safety. Together with the trend for more activities to be conducted electronically, thereby leaving a record, the overall effect is to create a much greater pool of available information that can subsequently be searched in relation to particular individuals, or, even more significantly, matched to *identify* individuals of interest.

There is a key difference between access to information in ad-hoc investigations by government agencies, and routine reporting and compilation of databases. The analysis in this paper focuses particularly on the latter – often resulting from statutory obligations to identify customers, maintain records and/or routinely pass bulk information to government.

Another significant trend has been a clear reduction in the level of transparency and oversight. An important contextual factor is, since July 2005, government control of the

Senate[1] for the first time in 30 years – there is now far less parliamentary scrutiny of legislation and of the Executive's exercise of powers (through Senate Committee processes). This is mirrored at State level by government control of all State/Territory parliaments – there are currently no 'hung' parliaments able to act as a constraint on Executive power.

While some new accountability mechanisms have emerged in recent years in response to 'scandals' (notably anti-corruption and police integrity agencies), other accountability mechanisms such as parliamentary committees, Ombudsmen, Privacy Commissioners and other 'watchdogs' have been weakened either by limitations on independence or scope and/or by resource cutbacks. Another example is the loss of *judicial* oversight of various warrant processes – illustrated further below.

The general position on government access to information

Before answering the specific questions it is necessary to state the general position of access by government authorities to personal information held by businesses and other organizations, where no special laws or rules relating to particular activities apply.

The general position is that the police and many other government agencies may *request* information from private sector organisations relating to customers or employees. It is then up to the recipient of that request to weigh up the public interest in co-operating against customer privacy. For those businesses subject to the Privacy Act 1988 (and in some states also health privacy laws) it would be a question of whether the requested disclosure fell under an relevant exception – the law provides for disclosure either where it is *required* by law (e.g. with a court order or search warrant)[2] or at the discretion of the organization where it is either authorised by law or to assist law enforcement or revenue protection.[3] Similar provisions are found in the state health privacy laws that apply to some private sector and non-profit organisations[4].

For the many organisations not subject to any privacy laws (e.g. most small businesses, and all businesses in relation to employee records), the decision to release information is discretionary, and many are likely to co-operate without giving privacy much thought, although HR policies would probably constrain many employers.

A disclosure could be *'required'* by law as a result of either a court order (such as a subpoena), a search warrant, or a statutory notice – many government agencies have powers to require information (without any independent warrant) in pursuit of their particular functions – including federal and state tax offices, regulatory and licensing

[1] The upper house of the Commonwealth (Federal) Parliament
[2] Exception at NPP 2.1(g) in the *Privacy Act 1988, Schedule 3*
[3] Exceptions at NPP 2.1 (g) and (h)) (also other exceptions)
[4] The *Health Records Act 2001* (VIC), the *Health Records and Information Privacy Act 2002* (NSW) and the *Health Records (Privacy & Access) Act 1997* (ACT)

authorities, welfare and benefit agencies, health and safety regulators and a variety of 'watchdogs' and complaint handing bodies.

In late 2005, the Australian Federal Police were given new 'notice to produce' powers[5] which provides them with a means of access to information without a search warrant in relation to investigation of any serious offence, not just terrorism[6]. Significantly, the power overrides not only privacy laws but also legal professional privilege, duties of confidence and any other public interest[7], and also prevents someone served with a 'notice to produce' from informing any other person (other than those involved in responding, and the person' own legal advisers)[8]

Most search warrants are issued under the provisions of the criminal law in each jurisdiction. In most jurisdictions, they may be issued either by judges or magistrates, and the occupier of the premises being searched must be notified, preferably at the time of the search but if not then as soon as practicable afterwards.

Search warrants may also be obtained by the Australian Security Intelligence Organisation (ASIO) under its own legislation.[9] A new category of ASIO 'computer access warrant' was introduced in 1999, providing for using equipment and manipulating and copying data as well as initial access to relevant premises.[10] In relation to computer data, see the discussion of encryption under telecommunications below.

Government agency databases

Apart from the annual reports and websites of individual agencies, a good source of information on the overall range and type of record systems held by Commonwealth agencies is the Personal Information Digest published each year as a requirement of the Privacy Act 1988.[11]

All Australian Police Forces, taxation authorities and other investigative and enforcement agencies keep their own files and databases, and there are many bilateral and multilateral information sharing agreements. However, there is also a central agency CrimTrac which holds a range of data as a common resource for specified agencies. According to the agency:

> "CrimTrac holds a National Names Index (NNI), which comprises multi-jurisdictional indexed data on Criminal Histories, Missing Persons, Warrants, Domestic Violence Orders, Adverse Firearms History and other related information on persons of interest for police nationally. Each jurisdiction remains

[5] Crimes Act 1914, Part 1AA, Division 4B, amendments made by the Anti-terrorism Act (No. 2) 2005 no. 144, 2005, Schedule 6
[6] Crimes Act 1914, ss.3ZQN and 3ZQO
[7] Crimes Act 1914, ss.3ZQR
[8] Crimes Act 1914, ss.3ZQT
[9] Australian Security Intelligence Organisation Act 1979, s.25
[10] *Australian Security Intelligence Organisation Act 1979*, s.25A
[11] Personal Information Digest (Commonwealth) (PIDC) 2005 at http://www.privacy.gov.au/publications/index.html#P

> responsible for its data and updates the NNI on a regular basis. The index of records is kept indefinitely. Only the police jurisdiction that created a record can amend/update/delete it."[12]

NNI enquiry volumes rose from 3.7 million enquiries in 2001-02 to more than 5 million in each of the last two years.[13]

Use of information obtained using statutory powers

Government agencies generally appear to consider any information lawfully obtained as 'fair game' for any subsequent lawful function. Moreover, the cumulative effect of the various statutory disclosure provisions is that information obtained by one agency for a specific purpose becomes at least potentially available to a range of other agencies for quite different purposes.

Information privacy laws, in those Australian jurisdictions which have them[14], purport to limit use and disclosure to the purpose for which information is obtained, but this principle is substantially undermined by the many exceptions, including where 'required or authorised by law' and 'where reasonably necessary for [a range of public purposes]'.

A 1993 High Court case[15] held that information about an individual obtained by the corporate regulator through use of a statutory demand power could not be disclosed to another agency for another purpose, at least without giving the individual concerned an opportunity to argue against disclosure. However, what seemed at the time to be an important constraint does not seem to have inhibited agencies in their creative use and exchange of information, and there has been no significant follow up either in other court cases or by the various Privacy Commissioners in their guidance.

Australian information privacy laws do not in practice have a significant limiting effect on the type and amount of surveillance by government agencies. They serve more to ensure a minimum level of transparency and procedural fairness, as well as to require minimum standards of data quality and security. The limits of surveillance are determined far more by the availability of information in relation to different aspects of individuals' lives and the powers of agencies under other laws to access that information.

This paper does not deal with powers of questioning and detention both under the ASIO Act and under the general criminal code – there have been major and controversial changes to these powers in recent years.

---

[12] Crimtrac entry in the PIDC 2005

[13] Crimtrac website - http://www.crimtrac.gov.au/aboutus.htm

[14] The Commonwealth, NSW, Victoria, Tasmania and the ACT and Northern Territory. The other states, Western Australia, Queensland and South Australia, do no yet have information privacy laws although they do to varying extents embrace privacy principles as administrative instructions.

[15] JOHNS v. AUSTRALIAN SECURITIES COMMISSION AND OTHERS [1993] HCA 56; (1993) 178 CLR 408 F.C. 93/041

Access to Communications

Regulation of communications is, under the Australian Constitution, reserved for the Commonwealth (federal) government, although this generally applies only to communications in transit – before dispatch and after delivery communications are subject to the same access powers as apply to other documents including State laws.

Postal communications

Letter post is still a state monopoly delivered through the corporatised but still wholly government owned Australia Post. The postal legislation[16] makes a distinction between 'articles' (letters, packages, and messages – including electronic messages[17]) and other information or documents. There is a strict prohibition on opening or examining articles, but with exceptions for a range of purposes[18]. Other information, including information obtained from examining but not opening articles (such as addresses) is also subject to non-disclosure rules, but with a broader range of exceptions[19], although penalties for unauthorised disclosure are the same for both.

Customer identification

Until recently, the only information about the sender of articles recorded by Australia Post was on customs declarations where they applied, or for premium services such as recorded or registered mail. The amount of detailed information about communications has however expanded dramatically with the introduction of new requirements to provide proof of identity when sending some overseas mail[20]. This information, which is held electronically for 90 days, is subject to the less stringent protection regime.

Australia Post maintains a National Address File containing all delivery addresses in Australia. While there is no automatic recording of named individuals at every address, change of address requests have over time built up into a substantial database of name

---

[16] *Australian Postal Corporation Act 1989*

[17] Australia Post offers a range of electronic transaction services. The exact relationship between the postal and telecommunications legislation as they apply to these services is unclear.

[18] *Australian Postal Corporation Act 1989* Part 7B, Divisions 3 & 4, which provide exceptions for Australia Post itself in relation to undeliverable articles or where there is reasonable suspicion of drugs, dangerous goods etc or of non-payment of customs duty

[19] *Australian Postal Corporation Act 1989* Part 7B, Division 2 – apart from s.90J, discussed separately, the protection under Division 2 equates broadly to the Use and Disclosure Principles in the *Privacy Act 1988*, which allow, for example, disclosure where reasonably necessary for revenue protection.

[20] Since December 2002, Australia Post customers are asked to provide proof of identity (POI) when lodging overseas bound mail (correspondence weighing more than 500 grams) is exempt, to meet Department of Transport and Regional Services requirements for enhanced security measures for international air cargo (Regulation 49 of the Air Traffic Regulations 1943 (Cth) . While not strictly required, anyone declining to provide POI is warned that their mail may be subject to 'security related ' delays (by implication, opening and inspection). There have been reports of Australia Post staff asking for POI for items under the weight threshold.

and related address information – over 9.6 million individuals in 2005.[21] There is also a database of more than 2.5 million post office box and private locked bag holders.

However, any information held by Australia Post, including about the substance or content of articles, is subject to an overarching disclosure authority[22], which allows disclosure in response to a Commonwealth, State or Territory warrant or court order; as *required* by any other Commonwealth law and certain specified State laws, to emergency services, and where there is reasonable suspicion of criminal law offences or of matters relevant to 'security'[23].

This amounts to a relatively weak non-disclosure regime for postal communications when compared to the equivalent law on telecommunications interception (see below). A wide range of information, including about communications content, is accessible without warrant.

Australia Post is required to report annually on the number of disclosures under the various provisions of the Act.[24] Reflecting the analysis above, in 2004-05 there were only 34 disclosures under warrant (to five different agencies) [23 in 2000-01[25]], and 95 without warrant to ASIO [204 in 2000-01], but more than 30,000 to a wide range of government agencies under the alternative 'authorised by law' provisions[26] [17,000 in 2000-01]. There is no breakdown given of how many of the disclosures involved 'content' information.

Private delivery services

Private courier or delivery services, which now have a significant share of the total market for business letters and packages are not specifically regulated, and are therefore subject to the same laws as other businesses in relation to access by authorities. ASIO has equivalent warrant powers in relation to 'delivery service articles' as it does to postal articles[27], while other government agencies, including police, would use their general powers to request or require information from private delivery services.

Telecommunications

Protection of the privacy and confidentiality of telecommunications has until 2006 been characterized by a fundamental distinction between 'content' – regulated by the federal *Telecommunications (Interception) Act 1979* (TIA) and other information, including

[21] Australia Post entry in the PIDC 2005
[22] *Australian Postal Corporation Act 1989*, s.90J
[23] Security in terms of the *Australian Security Intelligence Organisation Act 1979,* s.27 which provides for warrants, issued by the Attorney-General for inspection by ASIO of postal articles in relation to specified addresses
[24] *Australian Postal Corporation Act 1989*, s.43(1)(n)&(o)
[25] Australia Post Annual Report 2000-01, Financial and Statutory Reports p.87
[26] Australia Post Annual Report 2004-05, Financial and Statutory Reports p.115
[27] *Australian Security Intelligence Organisation Act 1979,* s.27AA

transaction details such as call charge records – regulated by the *Telecommunications Act 1997*(TA).

Customer identification

Telecommunications legislation requires telcos (used in this paper to cover both carriers and carriage service providers, which include Internet Service Providers) to collect certain prescribed information, including subscriber name and address, from both fixed line and mobile (cellphone) customers, which is then required to be input to a central Integrated Public Number Database (IPND) - currently managed by Telstra under a licence condition and contract.

The IPND directly services emergency services operators (for response to 000 calls) and a range of law enforcement agencies, and also provides the feed, under prescribed rules and limitations, to producers of public directories. The compilation and use of the IPND is governed not only by provisions in the TA and carrier/CSP licence conditions but also by a mandatory binding Code[28]. Concerns about commercial uses of IPND data led the regulator in 1994 to propose issuing a binding Standard to replace the Code, and a draft Code was issued for comment in 2005.[29] While the final Standard has yet to appear, it is unlikely to effect access by government agencies to the IPND.

Identification of pre-paid mobile phone customers

At the close of the 2004-05 financial year, pre-paid services accounted for approximately 51 per cent of the 16.5 million mobile services currently in operation in Australia and represented the major area of growth in the mobiles market[30] (according to press reports the equivalent figure in Europe is 68%).

Production and recording of evidence of identity when opening a pre-paid mobile account has been required by law since 1997[31] but is not implemented or enforced across the board. According to the regulator, ACMA, in a recent consultation paper:

> "Mobile phones have typically been sold through a wide range of outlets, with activation carried out as a separate activity. Failure to collect the required information, discrepancies between information collected at point of sale and point of activation, and the lack of an accessible data source for identity verification all contribute to poor quality data going into the IPND, causing difficulties for emergency services, law enforcement, revenue protection and national security agencies." [32]

---

[28] ACIF C555:2003 *Integrated Public Number Database (IPND) Data Provider, Data User and IPND Manager*
[29] See http://www.acma.gov.au/ACMAINTER.131402:STANDARD::pc=PC_6124
[30] Australian Communications and Media Authority, Discussion Paper: *Improving Identity Check Processes for Pre-paid Mobile Services*, March 2006
[31] See http://www.acma.gov.au/ACMAINTER.131402:STANDARD::pc=PC_1899
[32] ACMA Discussion Paper, March 2006

A 2005 audit of the IPND by ACMA found that only 35.2 percent of mobile service records were categorised as 'highly accurate' compared to 79.3 per cent of fixed service records.

The current consultation by ACMA is likely to lead to tougher requirements and greater enforcement, resulting in more complete databases of mobile phone customers, feeding into the IPND.

Identification of callers

Calling line identification (CLI) is transmitted between telcos as a necessary part of providing telecommunications services. CLI is also the basis of Caller Number Display (CND) services which allow call recipients to display the number (and in some cases the name) of the caller. CND services were introduced in Australia in the mid 1990s on an opt-out basis – lines are set to transmit CLI so that it can be displayed as CND by the recipient, unless the customer expressly opts out. They can choose to 'block' CND either on a call-by-call basis by dialing an override code (per-call blocking) or as a permanent setting for their line (line blocking). Unlisted (Silent line) customers (approximately 1.7 million) are given a line block by default. Calls to *emergency services* transmit CLI whether or not there is a line-block in place or the caller has activated a per-call block. However, *law enforcement agencies* seeking, for non-emergency response purposes, to ascertain the number from which a particular call was made, where that number had been 'CND blocked', would have to go to the relevant carrier with a Part 13 request (see below).

The range of government enforcement agencies which have authorised access to the IPND are able to use a 'reverse search facility' to look up the name and address of the subscriber of the line (or mobile phone) from which any particular call is made, if they have obtained the number, either through CLI or by other means. Public reverse search directories are not allowed under the Act and IPND Code, although products that allow reverse search have been available from time to time – either exploiting loopholes in the law or defying the restriction.[33]

Retention or preservation of telco records

Telcos have traditionally kept transaction records, linked to customer details, only for as long as they needed to for commercial reasons (such as billing and dispute resolution). This is consistent with one of the principles found in most information privacy laws.[34] A debate started in Australia in the late 1990s about retention periods for records held by Internet Service Providers (ISPs), prompted partly by the parallel development of a Council of Europe Cybercrime Convention[35]. The Internet Industry Association developed a draft Code of Practice which was issued for public consultation in 2003[36].

---

[33] In May 2006, ACMA and the Privacy Commissioner both launched investigations into two websites offering reverse search functions.

[34] Many such laws require destruction or de-identification of personal information once it is no longer required – e.g. NPP 4.2 in the *Privacy Act 1988*

[35] Council of Europe Convention No 185 on Cybercrime, 2001 (entered into force 2004)

[36] Internet Industry Association Draft Cybercrime Code of Practice v.2 July 2003 - http://www.iia.net.au/

The draft Code proposed that ISPs keep records for either six or 12 months (depending on the type of information) to meet the potential needs of law enforcement agencies. The Code has not progressed and it is not known to what extent ISPs have changed their retention practices in response to the draft, or to reflect development in other jurisdictions concerning either routine retention or alternatively preservation of specific records on request.[37]

Access to telco information other than content

Whatever the retention period, government agencies will have an interest in accessing telco records for a variety of purposes. Apart from interception of content (see below), access by government agencies to other personal information held by telcos, including call charge records (numbers connected, time and duration of a call) would be under Part 13 of the Telecommunications Act. This Part generally prohibits disclosure without the customer's consent but expressly authorises a range of disclosures including to specified law enforcement and revenue protection agencies. Unlike most other private businesses, telcos are also under a specific obligation to give assistance to these agencies, under Part 14 of the Act.[38] Part 13 provides for agencies to provide certificates of 'reasonable necessity' that telcos can rely on, but also allows them to make 'discretionary' disclosures without a certificate.

The volume of disclosures under Part 13 is publicly reported.[39] In 2004-05, telcos made 885,000 disclosures in total (733,000 in 2000-01), comprising 280,000 criminal law certified (163k); 400,000 criminal law uncertified (440k); 88,800 revenue protection certified (15k), 1775 pecuniary penalty certified (3k), and 15,649 RP & PP uncertified (88k).[40] This means that in 2004-05, 59% of all disclosures for criminal law purposes were uncertified, whereas only 15% of revenue protection disclosures were uncertified. Note that telcos appear much more willing to assist criminal law enforcement than revenue protection agencies without the re-assurance of a certificate (perhaps reflecting the Part 14 obligation), and the dramatic reversal of the ratio of uncertified to certified revenue protection disclosures since 2001. Records of certified disclosures are audited by the Privacy Commissioner[41], while telcos only have to report the numbers of the different categories of uncertified disclosures to the ACA (now ACMA)[42].

---

[37] There have been major debates about retention of telecommunications records both in Europe – see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp119_en.pdf and in the US, where government agencies can require telcos to preserve records pending the issuance of a court order or other process (Title 18, United States Code, Section 2703(f)) – see http://www.usdoj.gov/criminal/cybercrime/mmrArt29DRstmt041405.pdf

[38] *Telecommunications Act 1997*, Part 14

[39] The ACA is required under clause 50(2)(g) of the *Australian Communications Authority Act 1997* to report the number of disclosures made for the above purposes during the reporting period

[40] Australian Communications Authority, Annual Report 2004-05 - Table 25 in Appendix 9 and equivalent figures for 2000-02 from answer to Senate Estimates Committee question,

[41] TA s.309 - a limited monitoring of the record keeping requirements, not of the reasons for the requests.

[42] TA ss.306 and 308

It needs to be emphasized that these figures are for specific ad-hoc disclosure requests, over and above the bulk disclosure of personal information through the IPND and CLI, already described above.

Interception of telecommunications content (wiretapping)

Interception of telecommunications *during their passage over telecommunications systems* is federally regulated, by a purpose-designed *Telecommunications (Interception) Act 1979* (TIA). This Act has been the subject of regular review and amendment over the last 15 years, with major changes since 2001.

Most authorized access to the content of telecommunications is through Part VI warrants issued under the TIA[43] to designated law enforcement agencies (Australian Federal Police (AFP), Australian Crime Commission (ACC) and (currently 9) eligible State and Territory authorities declared under s.34) in relation to investigation of designated 'serious offences'[44]

Telcos (carriers) have been required under the *Telecommunications Act 1997* (TA) to develop and maintain interception capability[45] (during the 1990s this was very costly and was underwritten by government). A central AFP unit – the TI Division – carries out AFP interceptions and supervises the execution of interception warrants granted to other agencies.

Part VI warrants are issued by eligible judges or nominated tribunal members[46] (the latter only since a controversial change in the mid-1990s from federal judges only – the excuse was separation of powers although this has not stopped subsequent legislation giving executive functions to judges where it suits the government). It is convenient for government to use arguably less independent AAT members - in 04-05 only 192 warrants (7% of the total) were issued by the 21 eligible judges (and none by the 26 magistrates), while the 28 nominated AAT members issued 2691 warrants (93%).

Applications for Part VI warrants must be in writing giving reasons (there is provision for interim telephone applications/approvals where urgent), and the issuing authority is expressly required to have regard to privacy considerations.[47]

---

[43] *Telecommunications (Interception) Act 1979, Part VI*

[44] A previous distinction between Class 1 (mainly murder, kidnapping, narcotics and terrorism) and Class 2 (other serious) offences was removed by the Telecommunications (Interception) Amendment Act 2006, No 40 2006, Schedule 4

[45] TA Part 15

[46] Members of the Administrative Appeals Tribunal (mostly non-judicial members on short term appointments) appointed by the Attorney-General, and selected and nominated by the Attorney-General to exercise warrant-issuing powers

[47] This balancing requirement used to apply only to warrants for Class 2 offences but now that the Class 1-2 distinction has been removed by the 2006 amendments, applies to all warrants

Agencies must keep records which are subject to inspection by relevant Ombudsmen and AFP & ACC submit quarterly reports to the AG. The TIA specifies details which must be included in an annual report by the AG on the operation of the Act.

Approx 2800 Part VI warrants were issued in 2004-05 (down from around 3000 in each of the two previous years, but nearly a third more than the average before 2001.[48] About 1200 (44%) were in relation to Class 1 offences including 60 warrants for terrorist offences. Only 6 warrant applications were withdrawn or refused in 04-05 and 72 were issued with conditions or restrictions. Total recorded cost of executing warrants in 2004-05 (including capital expenditure) was approximately $30 million, with an average cost per warrant being in the range of $5000 - 20,000 for most of the eligible authorities. A recent Parliamentary Committee report cited a calculation that by comparison with the US for 2003-04, Australia issues 75% more warrants than the total number of US wiretap warrants, and that this represented 26 times the rate on a per capital basis.[49]

E-mail and message interception

A very significant recent change[50] has been amendment of the TIA to exclude 'stored communications' from the normal access regime of TI warrants. Stored communications are defined as those which have completed their 'transmission' over a telecommunications system and simply rest in electronic form awaiting action by the recipient. They include E-mails, SMS/MMS messages, pager messages and messages left on answering services. As a result of controversial amendments in 2006 (at the third attempt in recent years) these 'stored communications' are no longer protected by the requirement to obtain an interception warrant. They are instead now subject to a significantly less rigorous warrant regime.[51]

Other changes to interception law

Another controversial change is the provision for interception of so-called 'B-party' communications[52] - i.e. the communications of persons not themselves under suspicion, but in contact with a suspect. The use of this power clearly has enormous potential for surveillance of unsuspecting third parties. In partial recognition of this, the new provisions do involve a balancing test by the issuing authority and separate and specific

[48] 2157 Part VI warrants issued in 2000-01, 1689 in 1999-00, and 1284 in 1998-99 – source TIA Annual Reports

[49] Senate Legal and Constitutional Legislation Committee: Report into *Provisions of the Telecommunications (Interception) Amendment Bill 2006*, p.60 – citing media release from the NSW Council for Civil Liberties

[50] *Telecommunications (Interception) Amendment Act 2006*, No 40 2006, Schedule 1

[51] It should be noted that the stored communication regime was briefly even less rigorous – amendments in 2004 removed stored communications entirely from the TIA regime and left them only subject to the TA controls, but this was subject to a sunset clause. The 2006 amendments restored a warrant regime, albeit less rigorous than the Part VI regime.

[52] *Telecommunications (Interception) Amendment Act 2006*, No 40 2006, Schedule 2

reporting, but additional limits and safeguards recommended by a bipartisan Parliamentary Committee[53] were not adopted.

Another recent change is the introduction of 'named person' warrants[54] and equipment based interception[55], avoiding the need for applications to specify particular telephone services. In 2004-05 107 services were intercepted under 241 warrants served (398 issued?)

Intelligence agencies interception

The TIA provides separately for interception of telecommunications by the 'domestic' Australian Secret Intelligence Organisation (ASIO). These are issued by the Attorney-General[56] under a separate part of the TIA[57], and are therefore subject to even less 'independent' scrutiny than the Part VI warrants for other agencies. Warrants may be issued for ASIO's own investigations and also for interception by ASIO on behalf of the Departments of Defence or Foreign Affairs and Trade in relation to foreign intelligence (see below re 2001 incident). The number of warrants issued to ASIO is not publicly reported. The warrant regime is subject to the scrutiny of a nominally independent Inspector-General of Intelligence and Security who publishes an Annual Report. The recent provisions for named person warrants and 'B-party' interceptions, discussed above, also apply to the ASIO regime.[58]

In 2001, in connection with a highly controversial detention of a group of asylum seekers who had been rescued by a Norwegian merchant ship, it was alleged that the strict rules prohibiting interception of domestic communications by the Defence Signals Directorate (DSD[59]) had been breached. An investigation by the Inspector General of Intelligence and Security found four technical breaches of the rules in reports made to government by DSD, although there was no direct disclosure of any information about named Australians.[60] The Inspector-General made a number of recommendations designed to clarify the rules and ensure that they are followed in future.

Encryption

During the 1990's there was the same debate in Australia as elsewhere about the potential for encryption to frustrate legitimate government access to digital communications (and other data). The outcome, as elsewhere, was a reluctant acceptance by authorities that they are powerless to prevent the use of encryption by end-users, so that knowledgeable

---

[53] http://www.aph.gov.au/senate/committee/legcon_ctte/ti/report/c04.pdf
[54] *Telecommunications (Interception) Legislation Amendment Act 2000*, No 63 2000, Schedule 2
[55] *Telecommunications (Interception) Amendment Act 2006*, No 40 2006, Schedule 3
[56] The Act provides in s.10 for emergency warrants to be issued by the DG – limited to 48 hours
[57] *Telecommunications (Interception) Act 1979, Part III*
[58] *Telecommunications (Interception) Amendment Act 2006*, No 40 2006, Schedule 2
[59] Australia's equivalent of the US National Security Agency (NSA) or the UK Government Communications Headquarters (GCHQ).
[60] MV Tampa, August-September 2001 - Collection and reporting of intelligence relating to Australians: A report by the Inspector-General of Intelligence and Security, April 2002

users, including terrorists and other criminals, can conceal the content of communications, thereby limiting the value of interception. However, telcos providing digital services which offer encryption (including all GSM mobile services) are required by law to provide the authorities with the ability to de-crypt traffic that is only using the telco provided encryption[61].

The ability of individuals to protect their privacy through encryption is weakened by removal of the right to silence for persons suspected of criminal offences – the Queensland government is giving police the power to direct the handing over of encryption details and making it an offence to withhold these details.[62] This power is reportedly already enacted in the federal Crimes Act.[63][check]

Financial surveillance

Of all the areas of information privacy, financial privacy is generally highly valued. Individuals typically consider their financial affairs – assets and liabilities, income and expenditure – as particularly sensitive, and 'none of anyone else's business'. This concern is reflected in traditional concepts of banking secrecy. Yet paradoxically, the reality is that the requirements of modern life – in relation to both commerce and government – mean that our financial affairs are arguably ably more open to monitoring and reporting than many other aspects of our lives. In recognition of this reality, financial details are not even included in the definitions of 'sensitive information' in many Australian privacy laws.

'Customer' Identification

Monitoring of financial affairs starts with identification of individuals when they enter financial relationships.

When individuals enter employment, the employer is supposed to get them to fill out an employment declaration, in which the individual identifies themselves and gives their tax file number allocated to them by the Australian Taxation Office (ATO) when they first entered the workforce. This information is required to be reported to the ATO. While this should in theory result in a comprehensive database of all working Australians, the system is far from perfect or universal – there is a significant black economy and many false or duplicated tax file numbers – successive inquiries and audits have highlighted major weaknesses in the TFN system.[64]

---

[61] A requirement to provide 'special assistance capability' as well as general interception capability was inserted into the TA by the *Telecommunications Legislation Amendment Act 1997*

[62] Police Powers and Responsibilities and Other Acts Amendment Bill 2006 (QLD).

[63] Australian newspaper 6 June 2006

[64] Including the House of Representatives Economics, Finance and Public Administration Committee report: *Numbers on the run: Review of the ANAO audit report No.37 1998-99 on the management of Tax File Numbers*, August 2000

Financial institutions and other 'cash dealers' are required to identify customers under the *Financial Transaction Reports Act 1988* (FTRA). The FTRA was introduced as a measure to combat money-laundering and other serious and organized crime but has developed into a much wider scheme with multiple objectives. The Australian Transaction Reports and Analysis Centre (AUSTRAC) – a Commonwealth government agency - issues detailed Guidelines on customer identification, one of which specifies a points value for a wide range of 'evidence of identity' documents.[65] Persons wishing to open a new account have to meet a specified points score to satisfy the organization as to their identity, and the details are required to be recorded. Additional customer identification and reporting requirements for international funds transfer instructions and for bearer negotiable instruments were added by the *Anti-Terrorism (No2) Act 2006.*[66] Under currently proposed replacement legislation[67] the identification requirements will be significantly extended to a much wider range of business transactions, including lawyers, accountants, jewelers, and in due course, real estate agents.

The customer identification requirements under both Taxation and anti-money laundering legislation provide the foundation for extensive schemes of routine financial surveillance and reporting.

The customer identification requirements of the FTRA overlap with 'due diligence' or 'know your customer' requirements under the *Financial Services Reform Act 2001*. These requirements, which apply to businesses such as insurers and financial advisers which are not covered by the FTRA, are designed primarily for consumer protection – to provide a sound basis for any financial advice[68], but have the incidental effect of creating detailed records of individuals' financial circumstances which can then be accessed by government agencies under their general powers. Records have to be kept for at least seven years.[69]

Transaction reporting

All employers and financial institutions in Australia are required to report all earned and unearned (investment) income to the federal Australian Taxation Office (ATO) under the provisions of the *Income Tax Assessment Act 1936*. The ATO uses the system of tax file numbers (TFNs) already described to match returns against each other to determine gross income, and against individuals' tax returns to assist in calculation of tax payable. Any discrepancies are taken up with the taxpayer.

---

[65] http://www.austrac.gov.au/text/guidelines/guidelines/guid3.html
[66] *Financial Transaction Reports Act 1988* Part 2 Division 3A and Schedule 3AA
[67] Revised Exposure draft Anti-Money Laundering and Counter-Terrorism Financing Bill 2006 – see http://www.ag.gov.au/agd/WWW/agdhome.nsf/Page/RWP8B2E91AF7CF4CFCACA2570C900112F4C
[68] Australian Securities and Investment Commission, Policy Statement 175.80(a) "the providing entity must make reasonable inquiries about the client's relevant personal circumstances" -see http://www.asic.gov.au/asic/pdflib.nsf/LookupByFileName/ps175.pdf/$file/ps175.pdf
[69] Policy Statement 175.93

The TFN system was significantly upgraded in 1988, accompanied by the *Privacy Act 1988*, which contains a separate protective regime for the handling of tax file numbers.[70] The use of TFNs was subsequently expanded to cover welfare benefit administration, but with additional privacy safeguards, through the *Data-matching Program (Assistance and Tax) Act 1990*. There have been several subsequent minor amendments to the TFN and data-matching regimes. The Commonwealth Privacy Commissioner has specific monitoring responsibilities in relation to these regimes and reports on them annually.[71]

Apart from the routine reporting already described, the ATO and other regulatory agencies have extensive statutory powers to require information in connection with their functions.[72] These powers are routinely exercised by some agencies not just in relation to specific investigations but also to obtain records in bulk for data-matching purposes. Apart from the statutory data-matching program already mentioned above, the ATO conducts many other data-matching activities, as do social welfare and other agencies. Most of these have agreed to follow non-mandatory guidelines issued by the Privacy Commissioner[73] and brief reports appear in the Commissioner's Annual Reports.

There are specific exceptions to the taxation secrecy laws in favour of a range of law enforcement and intelligence agencies investigating serious crime.[74] The powers of the Australian Crime Commission (ACC) to access financial records in a major tax evasion and money-laundering investigation recently withstood a High Court challenge[75].

In addition to the routine reporting of income to the ATO, the *Financial Transaction Reports Act 1988* (FTRA) requires 'cash dealers' to report significant cash transactions (defined as greater than $10,000), *all* international funds transfer instructions, international currency transfers of more than $5,000) and any 'suspect'[76] transactions to AUSTRAC.

In 2004-05, AUSTRAC received more than 12 million reports, an average of more than 48,000 a day.[77] These comprised more than 2.2 million significant transaction reports (up from 1.6 million in 2000-01; more than 10.2 million international transaction reports (6.1 million in 2000-01); 26,000 international currency transfers (similar in 00-01).

There were 17,212 suspect transaction reports (an increase of 49% on the previous year, and up from 7247 in 2000-01). For more than 5000 of the suspect reports the reason for

---

[70] For the current Tax File Number Guidelines, issued by the Privacy Commissioner, see http://www.privacy.gov.au/business/tfn/index.html
[71] Office of the Privacy Commissioner, Annual Reports – see www.privacy.gov.au
[72] E.g. *Taxation Administration Act 1953*, s.65
[73] Office of the Privacy Commissioner: The use of data matching in Commonwealth administration – Guidelines, February 1998 - at http://www.privacy.gov.au/publications/HRC_PRIVACY_PUBLICATION.word_file.p6_4_23.15.doc
[74] *Taxation Administration Act 1953*, ss. 6C-6F
[75] See http://www.crimecommission.gov.au/content/media_rel/2006/060519-Ongoing%20Operation%20Wickenby.doc
[76] The criteria for assessing a transaction as suspect are very broad and highly subjective.
[77] AUSTRAC Annual Report 2004-05

the suspicion was classified as unspecified 'suspicious behaviour', highlighting the subjective nature of the assessments.

AUSTRAC databases are available on-line to more than 30 partner agencies – both Commonwealth and State and Territory agencies, mostly just law enforcement and tax authorities but also, since 2004, the major social security benefit agency, Centrelink and the income transferring Child Support Agency. In 2004-05, more than 2500 individual officers in those agencies had online access, and logged on more than 156,000 times, making more than 2 million searches – a 68% increase over the previous year. AUSTRAC also undertakes proactive analysis of its data, resulting in 2004-05 in 966 financial intelligence assessments, 787 of which were passed on to partner agencies, as well as 22,497 disseminations of suspect transaction reports (72% of these were to the Australian Taxation Office).

Credit reporting

One of the largest and most comprehensive private sector databases on individuals is that held by the major consumer credit reporting agency Baycorp Advantage (Baycorp).[78] Other credit reporting agencies including Dun & Bradstreet operate in Australia but focus more on commercial credit reporting. Baycorp holds both publicly available information such as court records of debt judgments and bankruptcy listings, and information about credit applications and defaults provided by subscriber businesses.[79] Credit reports, drawing on all the databases are then sold to subscribers to assist them in making decisions on loan applications. The operation of the credit reporting system is highly regulated under a separate Part (IIIA) of the Privacy Act 1988, which together with a Code of Conduct issued by the Privacy Commissioner places strict limits on what information is included[80] and who can obtain access.[81] Government agencies are expressly prevented from becoming subscribers, and they therefore have to exercise their general powers if they wish to obtain information from the Baycorp database.

Unlike in many other countries, so-called 'positive' or full-file credit reporting is not currently permitted, so the consumer credit databases do not comprise a comprehensive record of an individuals' credit transactions and repayments. The Privacy Act was extended to cover credit reporting as a direct response to a proposal for 'positive reporting' in 1989, and business groups periodically campaign for amendments to allow full-file reporting. Dun & Bradstreet have recently called for the financial industry to make submissions to a two year review of privacy laws by the Australian Law Reform Commission in favour of a form of full file reporting. Consumer groups have been

[78] See http://www.baycorpadvantage.com/home/home_default.aspx
[79] Some of the terminology in Baycorp's credit reporting operation reflects its origins as a mutual enterprise.
[80] Credit information files typically comprise names, address(es), date of birth, occupation, employer, and drivers licence number – the latter expressly allowed to assist in identification and matching of records, as well as types of loan applied for and enquiries from subscribers.
[81] See http://www.privacy.gov.au/business/credit/index.html

consistently sceptical of the case for change, arguing that significant problems with the existing default reporting scheme need to be addressed first.

Record retention

Many businesses have traditionally kept customer transaction records for a period of time – typically seven years – to aid compliance with tax laws. This 'custom and practice' is increasingly being superceded by more precise statutory record retention requirements, such as 7 years for personal information forming the basis of financial advice[82]. The contrary requirement in National Privacy Principle 4.2 of the Privacy Act to "… destroy or permanently de-identify personal information if it is no longer needed for [any legitimate] purpose …"[83] seems to have had little effect, as the plummeting costs of data storage allows organizations to keep more data for longer, 'just in case'.

Property information

Real Property transactions are recorded in State Land Registries, and are largely transparent through public registers, with no need for requesters to give reason for their interest, although there are restrictions on commercial re-use. Most states and Territories have licensed a range of commercial providers to give on-line access to land title information.

Registration of personal property securities, covering interests (including leases, hire purchase and retention of title arrangements) over most types of tangible and intangible personal property, is currently fragmented and inconsistent. There are currently moves to set up a more comprehensive national register, consistent with international standards.[84]

Shareholdings and directorships of public companies are similarly publicly available, the former directly from company share registrars[85], and the latter through registers administered by the Australian Securities and Investment Commission (ASIC)[86]. Controversy over unrelated secondary uses of share registers has led to statutory restrictions being placed on the use of the registers.[87] These have however proved difficult to enforce.[88]

Government agencies are able to access any public registers in the same way as members of the public, but in some cases have negotiated expedited means of searching and accessing public records. The ability of the custodians to make special arrangements for

---

[82] Australian Securities and Investment Commission, Policy Statement 175.93
[83] *Privacy Act 1988* Schedule 3, National Privacy Principle 4.2
[84] See http://www.ag.gov.au/pps
[85] The *Corporations Act 2001*, Chapter 2C
[86] See ASIC search page at http://www.asic.gov.au/asic/asic_srchlodg.nsf/byheadline/Home+Page?opendocument
[87] The *Corporations Act 2001*, s.177
[88] For an example of enforcement action by ASIC, see http://www.asic.gov.au/asic/ASIC_PUB.NSF/byid/AC85D287623EEE3ACA257133000ED6AA?opendocument

access by other government agencies varies and in some cases is constrained by the laws governing the registers, to the frustration of the agencies concerned, who keep up a general and constant pressure for preferential access arrangements[89].

Government benefits

For those many individuals in receipt of a government benefit, detailed records are kept and increasingly linked and matched, not only with each other but also with tax and other records, to police eligibility criteria and detect fraud and other abuses. Traditionally separate areas of public administration, such as health, welfare, education and transport are increasingly being integrated and data shared. This partly derives from interlocking eligibility criteria (e.g. public transport fare concessions for students and health benefit recipients) but also from a determination by governments to use whatever information is available in pursuit of efficiencies and to prevent fraud.

A national identity card?

The most recent, and highly controversial, manifestation of this trend is the proposal for a Commonwealth government health and social services 'access card'.[90] From the limited details made public, the government seems to envisage a new registration system for almost the entire population and the issue of a new smartcard to replace 17 different existing entitlement cards. Participation would be effectively mandatory (as it would be required to obtain health benefits which are available to nearly everyone) and this has led many critics to characterise it as a national identity card system 'by stealth'.

This perception has been strengthened by mixed messages from the government, which at various times has 'sold' the access card as the solution to everything from terrorism, through border security, welfare fraud, emergency medical treatment to natural disaster relief payments.

The merging or linkage of health information with information held for other purposes such as welfare or taxation is particularly sensitive. To date, there have been significant legislative, as well as practical, barriers to sharing and linking of health information, including detailed and specific provisions about access to medicare and pharmaceutical benefits scheme records[91], but these limits have been criticized and are currently under

---

[89] The same issues arise in relation to registers of electors, and of births, deaths and marriages, which are generally governed by laws requiring limited publication for public inspection but also prohibiting other forms of access and uses e.g. in bulk for commercial purposes. The tension between public accountability and privacy were explored by the Federal Privacy Commissioner in a 2002 Consultation Paper, which in turn led to Information Paper No 17: *Privacy and Personal Information that is Publicly Available*, 2003. See also the Victorian Privacy Commissioner's Guideline : *Public Registers and Privacy - guidance for the Victorian Public Sector*, Edition 1, August 2004

[90] Official material at http://www.humanservices.gov.au/access/supporting_information.htm For a comprehensive, though openly critical overview, see www.privacy.org.au

[91] National Health Act 1953 s.135AA and Privacy Commissioner Guidelines under that section – see http://www.privacy.gov.au/publications/mapbpg.doc

review.[92] The barriers around health information are coming under increasing incidental pressure as a result of government initiatives linking health care to other benefits and tax concessions, and they may in any case need to be relaxed if the proposed health and social services 'access card' (see above) is to operate as intended. It is increasingly difficult to separate surveillance of financial affairs from surveillance of other behaviour and attributes, including health.

There are numerous initiatives under way at both the federal and State/Territory levels in the areas of electronic health records, unique patient identifiers and data-linkage for both health research and administration.[93] Privacy concerns have loomed large in discussions of these initiatives, and prompted the issue for comment in 2002 of a draft national Health Privacy Code, but this appears to have stalled.[94] As in so many other areas, there is little doubt that, for sound reasons, more comprehensive databases of health related information will continue to develop but this will again provide a tempting resource for a range of government agencies pursuing non-health related interests.

Whatever other uses are made of the proposed 'access card', there is no doubt that a primary, and intended, effect will be to further extend the routine surveillance of individuals' financial affairs.

Tracking individuals' movements or location

International Travel

Information about individuals' movements in and out of Australia is held by the Commonwealth government using a combination of passport and visa records together with information supplied by transport operators. The central Movements System database currently contains more than 200million records, which are kept indefinitely.[95] A movement alert database contains records relating to foreign nationals and certain Australian citizens whose entry may be of concern to the Australian Community (some 190,000 individuals in 2005).

There has long been some exchange of information between airline and shipping operators and the Immigration and Customs agencies about crew and passenger movements, but in the past this was generally on an 'exception' basis.

Over the last few years, the amount of routine transfer of 'bulk' data about passengers in particular has increased dramatically. An unspecified number of records are held in an

[92] See http://www.privacy.gov.au/health/guidelines/healthreview.html
[93] For an overview of some of these initiatives, see http://www.nehta.gov.au/ and http://www.health.gov.au/internet/hconnect/publishing.nsf/Content/home
[94] See http://www.austlii.edu.au/au/journals/PLPR/2003/3.html
[95] See DIMIA entries in the PIDC 2005

Advanced Passenger Processing system, with a retention period of 12 months.[96] Australian authorities have co-operated with the US government in relation to the advanced provision of airline passenger data both for the US visa-waiver program[97] and the more general US border security initiatives. Australia has become caught up in the dispute between the US and EU authorities about passenger name record (PNR) data, with the EU questioning Australia's requirement for airline PNR data to be transmitted to the US authorities in the context of the EU's assessment of the adequacy of Australian privacy laws under the EU Data Protection Directive.[98]

Australia has also been an early adopter of the new ICAO standard for biometric passports, with a new e-Passport introduced in October 2005.[99] The government is also moving ahead with a face recognition system (Smartgate[100]) at selected airports. Critical questions have been asked in Parliamentary committees and more widely about the security, accuracy and reliability of both the e-Passport and Smartgate.

Most recently, the AFP and ASIO have been given a new power to require operators of aircraft and ships to disclose "information or documents (including in electronic form) that are relevant to a matter that relates to the doing of a terrorist act". [101] It is too early to say how broadly these new powers will be used, or even what level of public reporting there will be.

Domestic travel

There is no routine collection by government authorities of information about individuals' movements within Australia, although as described below, the amount of information being collected 'incidentally' as a result of various 'smart' transport initiatives is increasing rapidly, becoming a huge potential resource for government surveillance.

Toll roads

An increasing number of roads, bridges and tunnels in Australia are being financed by tolls, and the more recent ones[102] are being introduced without a cash payment option. Users have to either have an electronic 'tag' or purchase a period pass. There are no pre-paid anonymous tags – users have to open an account, and like purchasers of period passes, have to provide personal information. Digital images are taken of all vehicle

[96] See DIMIA entry in the PIDC 2005
[97] See http://usembassy-australia.state.gov/consular/visawaiver.html
[98] Correspondence between the Australian Privacy Foundation, the Australian Attorney-General, and the European Commission in 2004 - see http://www.privacy.org.au/Papers/index.html
[99] See http://www.dfat.gov.au/dept/passports/
[100] See http://www.customs.gov.au/site/page.cfm?u=4243
[101] *Crimes Act 1914* s.3ZQM, and *ASIO Act 1979* s.23
[102] Including several highways comprising the Melbourne City Link , and, in Sydney, the M2 and M7 motorways and cross city tunnel.

licence plates and matched either to account holders[103] or registered period pass holders. Even on those toll roads which do have a cash payment option, a majority of users are now using electronic tags[104], and are therefore subject to the same level of monitoring[105]. While some of the toll road operators are private, they operate under detailed government rules (in some cases specific legislation) which include provision for enforcement action for toll evasion by government agencies. Access by the enforcement agencies to the detailed records of vehicle movements is therefore 'built-in' to these toll schemes. The records are also potentially available to other government agencies for other purposes using their general powers, although in the case of the Melbourne City Link, the tracking issue was considered sensitive enough to justify specific legislative provisions regulating access to the records.[106]

Road & Traffic authority cameras

State and Territory governments maintain extensive networks of cameras both on major highways and in urban areas – both for traffic management, and to detect speeding and other traffic violations. Automated numberplate recognition (ANR) technology is increasingly being used to identify specific vehicles. The same authorities are generally responsible for vehicle licencing, so that images are effectively personal information about motorists travel history, and there is clear authority for police access to the records, not only for their role in enforcing traffic rules. Privacy Commissioners have expressed concerns about the potential for surveillance and use of the records for unrelated purposes. In NSW, the police have been unwilling to provide any meaningful information about the use of ANR technology.[107]

Vehicle location

According to a recent media report, there are some 100,000 Australians using vehicle tracking systems, and more than 1000 vehicles a month are sold with satellite navigation (satnav) systems fitted.[108] Most of these would be commercial fleet vehicles, although many luxury cars are now sold privately with satnav fitted, and there is also a growing market for satnav systems for retro-fitting to cars already in use. Commercial fleet users of satellite navigation systems increasingly use the information for management purposes, just as they did the earlier generations of tracking technology such as tachographs.

---

[103] For most account holders, where a valid e-tag transaction is recorded, the images are never accessed, but because the tags are associated with particular vehicles, the operators retain the images for a period of time, partly to allow them to enforce the account conditions.

[104] Press reports suggest more than 80% of movements on the Sydney toll roads still allowing a cash option now use the electronic tag/account option

[105] It is assumed that for vehicles whose drivers pay cash, an image of the licence plate is still taken, as toll booth lanes appear to be 'mixed'. If so, the only difference in tracking is that for 'cash' movements, there may not be a matching account, with an account holder's details attached. Government authorities obtaining access to images would still be able to match them to licensed vehicle owners.

[106] *Melbourne City Link Act 1995* (Vic), Part 4, Divison 3

[107] Letter from NSW Police to the Australian Privacy Foundation, 24 May 2005

[108] Sky-high sales as satellite navigation hits the road, Australian Financial Review, 30 May 2006.

Vehicle tracking systems will fall under the tracking devices legislation described below, meaning that they can only be installed with the express or implied consent of the person being tracked. Access by government authorities to both real-time and historic information from satnav systems would be through their general powers to access business records.

Public transport smartcards

The four most populous Australian States[109] are currently introducing smartcard based public transport fare systems, at least in their metropolitan areas[110]. These systems will in due course generate large amounts of transaction data which at least potentially will allow the movements of individual passengers to be tracked. In some cases the card systems are being expressly designed to perform other functions, including payment for small value items, which will significantly extend the scale and 'meaning' of the transaction database. The authorities involved are taking different approaches to the privacy issues involved, but there is little doubt that at least some government agencies will have some authorised access to these records.

Other location information

Mobile phone location

Telcos are currently able to locate mobile phone users by measuring direction and strength of signals to two or more base stations, but the precision of this location information varies widely with the density of base stations, and even in urban areas is no less than hundreds of meters. Mobile phones incorporating GPS technology are capable of much more accurate location finding, but there is no evidence that this detailed location information is routinely accessible to the telco providing the service.

An industry Guideline on mobile phone location information for emergency services was issued in 1999, specifying a system of Standardised Mobile Service Areas.[111] In 2004, the then ACA issued a discussion paper.[112] The ACA subsequently reported "It is expected that, at some point, carriers will introduce accurate location techniques and technologies into their networks when this becomes commercially attractive. Accordingly, the ACA does not propose to require carriers to introduce [the techniques] solely for providing emergency services with more accurate location information. The ACA instead intends to focus on preparing the emergency call service for the future introduction of these techniques and technologies, to ensure that ESOs can receive and use more detailed

[109] NSW, Victoria, WA and Queensland
[110] See for example http://www.tcard.com.au/tcardweb/ and http://www.doi.vic.gov.au/DOI/Internet/planningprojects.nsf/AllDocs/3B3484F49BFF94164A256F3300069890?OpenDocument and http://www.pta.wa.gov.au/scripts/viewoverview_contact.asp?NID=1264 and http://www.translink.qld.gov.au/qt/TransLin.nsf/index/TransLinkSmartCardSystem
[111] See http://www.acif.org.au/__data/page/3250/G530_1999.pdf
[112] Australian Communications Authority, Location, Location, Location, January 2004

location information to advantage once it becomes available." [113] Subsequent Annual Reports from the ACA/ACMA do not provide any further update on this issue.

Location of Financial Transactions

Financial institutions' records will show which Automated Teller Machines (ATMs) or Electronic Point of Sale (EFTPOS) terminals a customer has used, with dates and times. Stored value smartcards (such as those being introduced as public transport tickets) also have the potential to track the holder's movements through records of minor transactions.

Because the financial institutions themselves have had limited interest to date in individuals' location and movements, their systems are not generally configured to report on those characteristics. This has limited the value of such records to government agencies.

However, businesses are starting to explore the commercial value of location records both for analysis of customer behaviour and for direct marketing based on consumers' location and transaction patterns and characteristics, including location. Once businesses develop systems that make retrieval of location data easier, government agencies will also start to use their general powers to access such data where it is relevant to their functions, such as for criminal investigations.

Surveillance devices

The Federal parliament enacted the Surveillance Devices Act 2004 to provide a unified framework for the authorisation of the use of various surveillance devices – and superceding existing provisions in the Customs Act and Australian Federal Police Act. It is broadly based on a model surveillance device laws agreed with State governments.

Surveillances devices are defined in the Act as data surveillance devices, listening devices, optical surveillance devices and tracking devices. Surveillance devices may be used by officers from the AFP, the ACC, State and Territory police forces and non-police agencies, such as State anti-corruption agencies, generally for the investigation of offences which carry a maximum penalty of at least three years imprisonment, plus some other specified offences and purposes. The warrant authorising and accountability regime is modelled on the *Telecommunications (Interception) Act* provisions (see above). Authorising warrants can be issued by eligible federal judges/magistrates or nominated Administrative Appeals Tribunal (AAT) members (see discussion under TIA). The Act establishes a reporting and inspection regime which allows for scrutiny by the Ombudsman, the Attorney-General and the Parliament. Both the AG's overall annual report and reports by each participating agency must be tabled in Parliament.

However, optical surveillance devices, listening devices and tracking devices may also be used without warrant where the device can be installed and retrieved without entering

[113] Australian Communications Authority Annual Report 2003-04

premises, or interfering with a vehicle or thing without permission. Listening devices may also be used without warrant by a law enforcement officer who is a party to the conversation being monitored or recorded.

In the second half of 2004-05 (the Act only commenced in December 04) there were a total of 257 warrants applied for and issued, 90% to the Federal Police and the balance to the Australian Crime Commission.[114] There were no warrants applied for by state agencies, which would typically use their own surveillance warrant regimes unless there was a federal element to the crime. 33 authorisations were also granted by senior officers for use of tracking devices.

Use of listening and tracking devices by the Australian Security Intelligence Organisation (ASIO) is separately regulated under the ASIO Act.[115]

The *Anti-Terrorism (No2) Act 2006* amended the *Aviation Transport Security Act 2004* to require the development of a Code for the use of optical surveillance devices at airports and on board aircraft[116].

The States and Territories are also progressively updating their outdated listening devices laws to conform to the national model law.[117] In some cases however these laws offer a more limited protection than might appear, as they apply only to use of devices in private premises – their use in public spaces, by both government authorities as well as anyone else, remains largely unregulated.

CCTV

Closed circuit television (CCTV) or video cameras are typically installed by owners or occupants of premises for security purposes. Access to video images for law enforcement purposes has until recently been regulated in Australia in the same way as access to other privately held records.

In NSW, the state Department of Local Government issued CCTV Guidelines for the use of CCTV in public places in 2000[118] and reported on an evaluation of the Policy and Guidelines in November 2001[119]. The use of CCTV in workplaces in NSW was regulated by the *Workplace Video Surveillance Act 1998* (NSW) until 2005 when that Act was superceded by the more general *Workplace Surveillance Act 2005* (NSW)[120].

---

[114] Surveillance Devices Act 2004, Annual Report 2004-05
[115] *Australian Security Intelligence Organisation Act 1979*, ss.26-26C
[116] *Aviation Transport Security Act 2004* s.4 and Part 4 Division 10
[117] E.g. the *Surveillance Devices Act 1999* (VIC), *Surveillance Devices Act 1998* (WA), *Crime & Misconduct Act 2001* (QLD), Chapter 3, Part 6
[118] *Policy Statement and Guidelines for the Establishment and Implementation of Closed Circuit Television (CCTV) in Public Places*, at http://www.dlg.nsw.gov.au/Files/Information/CCTVImplement.pdf
[119] See http://www.dlg.nsw.gov.au/Files/Information/CCTV%20final%20report.PDF
[120] See a Short Guide to the Workplace Surveillance Act at http://www.lawlink.nsw.gov.au/lawlink/privacynsw/ll_pnsw.nsf/vwFiles/WSA2005ShortGuide.doc/$file/WSA2005ShortGuide.doc

However, in a contrary trend, the Council of Australian Governments (COAG) meeting on Counter-Terrorism in September 2005 committed to development of a national framework for the use of CCTV for counter-terrorism purposes, including a National Code of Practice for CCTV systems for the mass passenger transport sector.[121]

It seems unlikely that any arrangements for wider CCTV coverage or increased access will be confined to counter-terrorist purposes. The NSW government was reported in early 2006 to be considering accessing in real-time the thousands of cameras owned by banks, supermarkets and other private businesses. An audit was reported to be underway to identify all of the cameras across the state, their owners and points of contact, with gaps in coverage identified with the aim of getting cameras installed there[122].

Obeying the law

An important question applying to all areas of surveillance is the extent to which government agencies actually comply with the legal restrictions on their surveillance activities. Evidence of compliance can emerge from media investigations, individual complaints under Privacy and other laws, and own-motion investigations reviews and audits, by a range of official bodies including Privacy Commissioners[123], Ombudsmen, Auditors-General, Royal Commissions, Integrity and anti-corruption watchdogs and Parliamentary Committees.

The few reports to date expressly addressing privacy breaches have mostly been about 'unauthorised' access and use of personal information[124], or about inadequate security or data quality measures[125]. The only report to date about 'authorised' but allegedly unlawful access or use have been the case of DSD interception of telecommunications already discussed above.

The general accountability climate in Australia is not conducive to public exposure of unlawful behaviour by government agencies (as opposed to by individual employees). While there are Freedom of Information laws in all Australian jurisdictions, they have

---

[121] See http://www.coag.gov.au/meetings/270905/index.htm#Approach

[122] See http://www.safeguardingaustralia.org.au/News/31_Jan06.htm

[123] The Commonwealth and Victorian Privacy Commissioners have audit powers in relation to their public sector jurisdictions, and all both they and the NSW and NT Commissioners can also initiate 'own motion' investigations where there are allegations of privacy breaches.

[124] Such as the NSW Independent Commission Against Corruption (ICAC), which in 1992 published a damning report about a widespread illicit trade in personal information involving the Roads & Traffic Authority and NSW Police. See http://www.icac.nsw.gov.au/index.cfm?objectID=E29C3FBC-0A49-5F37-232CAFC080486CAD&NavID=262BA41B-D0B7-4CD6-F955BD8CEE4CDF37

[125] For example, the Victorian Privacy Commissioner's 2006 report into failures in security of police files http://www.privacy.vic.gov.au/dir100/priweb.nsf/download/27DAEE1EBC21E085CA257123000A3688/$FILE/OVPC_Report_0106.pdf . The Commonwealth Commissioner published reports of several own-motion investigations in the 1990s but these are not available on-line. Audit reports are no longer published separately (except one on websites – see http://www.privacy.gov.au/publications/wsr01.html) but summaries are included in the Annual Reports

been significantly weakened over the last 20 years, and resources for promotion and monitoring of FOI cut back. Governments have resisted or ignored recommendations from review bodies to strengthen the operation of FOI laws.[126]

The future

Positives

In June 2006, a report was published of an independent Security Legislation Review Committee[127], established under the provisions of a 2002 Act[128], to review six terrorism related Acts passed in 2002-03. The Committee is critical of several aspects of the laws, finding them to be a disproportionate response to the terror threat of terrorism, and recommending change and additional oversight and monitoring. However, the government has already rejected some of the Committee's key recommendations.[129]

Following two limited reviews of the *Privacy Act 1988* in 2005[130], the federal government has given a reference to the Australian Law Reform Commission (ALRC) to conduct a major Inquiry into privacy protection in Australia[131]. The ALRC will be co-operating with the NSW Law Reform Commission which has received its own reference from the State government to review the NSW privacy and related legislation, and also consider the merits of a tort of privacy[132]. Discussion papers are expected to be issued later in 2006.

Negatives

In the meantime, as already mentioned, the federal government has announced its intention to introduce a smartcard to replace a range of existing entitlement cards[133].

---

[126] There is still no response from the Commonwealth Government to a joint 1996 report by the Administrative Review Council and Law Reform Commission in 1996 Open Government – see http://www.austlii.edu.au/au/other/alrc/publications/reports/77/ALRC77.html and repeated criticisms by both Commonwealth and State Ombudsmen have been largely ignored (see for example http://www.ombudsman.gov.au/commonwealth/publish.nsf/content/mediarelease_2006_03 and http://www.ombudsman.vic.gov.au/CA256F2D00228847/Lookup/Final%5fReview%5fof%5fthe%5fFreedom%5fof%5fInformation%5fAct/$file/Final%20FOI%20report2.pdf and the 2001 Senate Committee report into the FOI Amendment (Open Government) Bill 2000 - http://www.aph.gov.au/senate/committee/legcon_ctte/completed_inquiries/1999-02/freedom/report/report.pdf .

[127] See www.ag.gov.au/slrc

[128] The *Security Legislation Amendment (Terrorism) Act 2002*, Section 4. The review provision was forced on the government by the Senate, which it did not control in 2002, and specifies the members of the Review Committee as a mixture of statutory 'watchdogs' and representatives of civil society organisations. The 2005-06 review was therefore unusually independent of the Executive.

[129] Attorney-General's Media Release 111/2006 15 June 2006

[130] Federal Privacy Commissioner, Getting in on the Act: *The Review of the Private Sector Provisions of the Privacy Act 1988*, March 2005; and Senate Legal and Constitutional References Committee, *The real Big Brother: Inquiry into the Privacy Act 1988*, June 2005

[131] See http://www.alrc.gov.au/inquiries/current/privacy/index.htm

[132] See http://www.lawlink.nsw.gov.au/lawlink/lrc/ll_lrc.nsf/pages/LRC_cref113

[133] See http://www.humanservices.gov.au/idc.htm

While the government denies that it will amount to a national identity (ID) Card, many commentators believe that it will be, given the almost universal proposed coverage of the population, the underlying registration database and the intention for the card to display a digital photograph of the cardholder.[134] There is as yet only limited information available about the proposed scheme, but it will almost inevitably lead to greater routine monitoring, surveillance and tracking of individuals' activities, transactions and movements. The government has refused to release privacy advice that it has received, including an independent privacy impact assessment, but has appointed a consumer and privacy taskforce (within the agency responsible), the terms of reference of which are unclear.[135]

Related developments include the commitment by all Australian governments in 2005 to a national identity security strategy, to "enhance identification and verification processes and develop other measures to combat identity crime". The strategy will include the development and implementation of a national document verification service to combat the misuse of false and stolen identities; and investigation of reliable, consistent and nationally interoperable biometric security measures.[136]

The proposed new Anti-Money Laundering and Counter-Terrorism Financing legislation already mentioned above, with a much wider scope and coverage even than the current FTRA regime, represents a major shift towards routine surveillance as opposed to ad-hoc investigation.

Further reading

Australian Privacy Foundation http://www.privacy.org.au

Caslon Analytics http://www.caslon.com.au/australiacardprofile1.htm#registration

12 A Kelvin Grove, Nelson Bay
NSW 2315 Australia
Phone: 02 4981 0828 and 0407 230342
Fax: 02 4984 0995
E-mail: nigelwaters@iprimus.com.au
Web:

[134] For a critical view, see http://www.privacy.org.au/
[135] See http://www.humanservices.gov.au/access/index.htm
[136] See http://www.coag.gov.au/meetings/270905/index.htm#Identity