LexisNexis™ Butterworths

PRIVACY LAW BULLETIN

Volume 3 Number 9
Print Post Approved 243459/00067

Information contained in this newsletter is current as at April 2007

Contents

DNA identification, privacy and the irrelevance of Australian law

Jeremy Gans
FACULTY OF LAW, UNIVERSITY OF MELBOURNE

The technique of DNA identification is now more than two decades old. It has become a routine part of the investigation of serious crimes and an increasing part of the investigation of routine ones in most developed countries, including Australia.

Like nearly all investigative techniques, DNA identification's purpose is to reduce or remove criminals' behavioural privacy. A criminal, even a cautious one, may find it hard to avoid leaving behind bodily tissue (such as hair on the floor, blood under someone's fingernails or skin cells in a fingerprint) at or around the time of a person's criminal behaviour. The DNA that is common to most of the cells in the person's body will permanently link them to that tissue. The link isn't perfect — DNA matches can be explained innocently — but, once identified, a person whose DNA appears to match the tissue can be investigated further.

DNA, like other natural identifiers, is anonymous. The privacy impact of DNA identification therefore depends on police access to records that link people to their DNA. The most common record of a person's DNA is their 'DNA profile', a set of (typically) 18 numbers, easily discerned in modern labs, that, while only a tiny fraction of the information in DNA, nevertheless generally varies from individual to individual. Contemporary police, armed with a known person's DNA profile, can use it to identify things that person may have done or places that person may have been, where those things can be discerned from human tissue collected and analysed by the police.[1]

DNA, like other natural identifiers, is anonymous. The privacy impact of DNA identification therefore depends on police access to records that link people to their DNA.

What police can learn from a person's DNA profile is subject to technological limits, resource constraints, investigative prowess and legal regulation. This article discusses the latter. All Australian parliaments

have enacted statutes purporting to regulate how police obtain DNA profiles and what they can do with them.[2] This article outlines the intrusions into Australians' behavioural privacy that remain lawful despite this legislation.

Who can be investigated?

The main way to obtain a known person's DNA profile is to obtain some of the person's bodily tissue, typically their saliva, hair (including the root) or blood, and analyse it in a lab. All Australian jurisdictions give the police the power to take one or more of these samples from many suspects and offenders (and some others.) However, the potential intrusion into Australians' privacy goes beyond these grants of power in three ways.

First, all Australian jurisdictions now permit police officers to apply their DNA sampling powers without judicial approval.[3] This leaves decisions about the scope of these powers in the hands of a party with a vested interest in obtaining a DNA profile. For example, many Australian statutes bar suspect DNA sampling unless the needs of the investigators outweigh the privacy rights of suspects; however, it is now usually the investigators themselves who make this judgment. The NSW Ombudsman has recently reported that auditing police decision making about DNA sampling orders on suspects was impossible due to the absence of records setting out the reasons justifying the order.[4]

Second, when no power is available to compel someone to provide a sample, all Australian police can rely on that person's consent to having a sample taken.[5] Moreover, most jurisdictions also permit police to rely on consent even when a power is available, with many suspects and offenders explicitly told that a refusal to consent may result in the use of force to carry out a subsequent DNA sampling order.[6] Where such a consent is supposedly obtained, the police do not need to (purport to) stay within the statutory limits for compelled sampling. Consent is the ostensible basis for around 95 per cent of suspect and offender DNA sampling in NSW, Australia's largest criminal jurisdiction.[7] While all Australian statutes demand that any consent to DNA sampling be 'informed', the procedures they mandate — mainly obliging police officers to tell the person what offence is being investigated, how the sample will be taken and the complex law on DNA databases — fall far short of the concept of 'informed consent' as it is applied in medical and human research ethics.

Finally, Australian police can lawfully obtain a person's DNA profile without either an order or consent. To do this, the police merely need to collect a person's bodily tissue from an item the person has touched, such as a cup, a cigarette butt or a handkerchief. Such objects may be obtained by surveillance of the person (for suitable items that they discard), by contriving scenarios that allow collection (such as conducting a drug test or tricking the suspect into licking an envelope), by awaiting bodily processes while the person is detained (such as using cutlery or a tissue) or by accessing existing depositories of bodily tissue (such as Guthrie cards[8]). Australian courts have upheld the broad legality of these methods on the basis that they fall outside of the scope of statutes on forensic procedures and (typically) do not infringe suspects' rights to property and bodily integrity.[9] There is no public data about the number of DNA profiles that police obtain in this way.

What can be investigated?

If the police have obtained a known person's DNA profile, then the extent of the intrusion into the person's privacy depends on which DNA profiles they compare it with. Many Australian jurisdictions expressly confine the police's use and disclosure of information obtained from forensic procedures to investigative purposes;[10] however, those purposes encompass potentially broad intrusions into privacy. If a known person's DNA profile is compared to all DNA profiles from tissues found at crime scenes, then the police can potentially learn of any of the person's behaviour, criminal or innocent, associated, accurately or not, with any crime, actual or apparent, at any time, past or future. The behaviour uncovered may include staying in a motel room, driving a car, littering a roadside, using a syringe, handling a weapon or having sex.

Under Australian legislation, all offenders and suspects whose profile is obtained by the police, consensually or otherwise, lawfully face this full loss of privacy. In the case of offenders, this is consistent with the rationales of offender sampling: offenders' reduced rights to privacy and their risk of recidivism. In the case of suspects, by contrast, this intrusion greatly exceeds the purpose of their original sampling, which was to investigate the offence they were suspected of committing.

On the other hand, all Australian statutes provide that the DNA profiles of people who 'volunteer' to assist in an investigation can only be used for the 'purpose' for which the profile was volunteered.[11] Despite this rule, many volunteers will still face a significant potential loss of privacy. For example, a profile volunteered to investigate a serial offence might be used to test the volunteer's links to all similar offences in the area. Moreover, volunteers can opt (or be asked) not to limit the use the police make of their profile. Finally, DNA profiles from victims of crimes of bodily violence may be treated as crime scene profiles, which are free of usage limitations. In 1999, this happened to a rape victim in Victoria, who was then wrongly linked to a notorious child homicide.[12]

A number of Australian jurisdictions have enacted further restrictions in the form of a table of permitted and forbidden 'matches' among defined database 'indices' (for example, profiles of relatives of missing persons) developed by a Commonwealth–state committee in 2000 as a legislative model to underpin a proposed national DNA database.[13] The practical impact of these restrictions is now doubtful. Among others, the Commonwealth, which administers the national database, recently repealed all usage restrictions on non-volunteer profiles, deeming them drafting errors or unnecessary.[14] It is likely that the remaining Australian jurisdictions will follow suit. The repealing legislation also clarified that the Commonwealth's statutory matching restrictions do not

apply to comparisons between DNA profiles held by different jurisdictions.[15] These will instead be governed by administrative agreements between the jurisdictions, contrary to a recommendation of the Australian Law Reform Commission.[16]

Moreover, no Australian jurisdiction bars police officers from keeping records of DNA profiles in places other than official DNA profile databases. Doing so is as simple as writing down a name and eighteen numbers on a piece of paper, which can then be kept in a filing cabinet or pinned to a bulletin board. While a DNA profile that isn't on a database cannot be easily compared en masse with other profiles, it can be compared on an ad hoc basis to other profiles known to an investigator. Except in WA (perhaps),[17] such profiles are not covered by rules regulating matching among database indices.

So long as a person's DNA profile is retained by the police, it can be used to identify their future behaviour, including conduct that occurs long after the sample was taken.

When can someone be investigated?

So long as a person's DNA profile is retained by the police, it can be used to identify their future behaviour, including conduct that occurs long after the sample was taken. Until recently, all Australian statutes except the NT's expressly required the destruction (or de-identification) of many DNA profiles obtained via forensic procedures after set time limits or other triggers (for example, an offender's successful appeal, the dropping of charges against a suspect, the conclusion of an investigation where volunteers gave samples), so that intrusions into some people's behavioural privacy would cease once the purpose of their original sampling had ended.[18] The rules are backed by criminal offences and, in most jurisdictions, provisions automatically excluding evidence derived from an illegally retained profile from courtrooms.[19] Alas, recent developments suggest that even these strong protections will do little in practice to protect Australians' behavioural privacy.

The major problem is that compliance with the destruction rules requires proactive steps by a number of state authorities. For every DNA profile obtained, police and prosecutors must track developments in that person's case and database administrators must link those developments (and the progress of statutory time limits) to every profile they hold and determine whether destruction is warranted (as the person may face other investigations). In WA, concern about the administrative burden led Parliament to make nearly all destruction requirements conditional on a request being made by the person sampled.[20] This transfers the responsibility for compliance to lay people, who may be unaware of the destruction rules or facts relevant to them and whose desire to be removed from the database might be treated by

some police as itself suspicious.

Elsewhere, the situation may be worse. In 2005, the SA Auditor-General reported that that jurisdiction's destruction rules, enacted in 2002, were not complied with for several years as a multi-year backlog developed due to a failure to agree on protocols for destruction or develop appropriate software.[21] In one high-profile case, a prosecution for armed robbery collapsed after DNA evidence sourced from a database match was excluded because the match was made after the defendant's profile should have been removed.[22] However, in a second case, there was no legal sanction because the defendant pled guilty.[23] No-one was prosecuted for non-compliance with the SA destruction rules. To the contrary, some parliamentarians labelled the court decision 'highly technical' and urged police to continue to ignore the rules pending the passage of retroactive legislation.[24]

The new SA legislation, passed early this year, signals the likely fate of statutory destruction rules across Australia. It has no destruction requirement for suspects' and offenders' DNA profiles, even if the suspect is never charged or is acquitted of the offence for which the profile was obtained.[25] This follows the pattern set in England, where a similar court case prompted the repeal of destruction rules not only for suspects, but also volunteers, whose consent to having their profile placed on the database is deemed irrevocable.[26] In both cases, the removal of destruction rules was justified, not only by administrative convenience, but also by the investigative benefits of permanently monitoring the behaviour of people even after the original purpose for their sampling had expired. Following public outcries about the permanent retention of DNA profiles from juveniles briefly arrested for minor crimes, the English regime was recently ameliorated to allow the ad hoc removal of profiles from the database at the police's discretion.[27]

Who else can be investigated?

So far, this article has outlined how police can lawfully obtain all Australians' profiles, can make extensive use of most of them and can — or, eventually, will be able to — keep most of them indefinitely. A significant recent development in investigative practice will mean that this already vast authority to intrude into Australia's behavioural privacy will be exponentially broadened.

Police in England have lately begun to trawl their database of known people's DNA profiles for partial, rather than full, matches to crime scene profiles.[28] A partial match, while excluding the known person as the source of a crime scene tissue, is an indication that one of that person's blood relatives may be the source. In one case, semen from a string of unsolved rapes was partially matched to the DNA profile of a woman, herself sampled after being arrested for drunkenness in the aftermath of an unrelated rape. After investigating her relatives, the police eventually arrested her brother, who pled guilty to the rapes.[29]

The investigative benefits of this practice are obvious, but so are the dramatic implications for Australians' behavioural privacy. If these so-called familial screenings become routine, then the police's existing lawful authority to obtain and use the DNA profiles of sundry offenders, suspects, volunteers and others will extend to all those people's close blood relatives. For example, in SA, if one person is temporarily suspected of a serious offence, then that person's siblings, parents, children and other close family members will permanently lose their behavioural privacy.

Except perhaps in the NT,[30] no Australian statutes bar the partial matching of DNA profiles from offenders, suspects, crime scenes and dead or missing persons.[31] The situation is less clear for people who volunteer their DNA profile for use in a 'limited purpose'. If people offer their DNA profile to eliminate themselves from an investigation, do they implicitly agree to the police using their profile to determine whether one of their blood relatives is the guilty party?

Conclusion

The balance between the investigative benefits of DNA identification and its

privacy implications is a matter for continuous debate worldwide. Some criticise the 'surveillance creep' of incrementally expanding police powers to gather and use DNA, while others propose that DNA profiles should be collected from everyone, citing the increased accuracy and non-discriminatory nature of a comprehensive approach.[32] The outcome of these policy debates may define the balance between law enforcement and privacy for the next few decades.

However, in Australia, legislatures have already given police the lawful authority to collect and use DNA profiles to an extent that approaches the broadest proposals for a uniform database. This was not a considered or even deliberate act, but rather the by-product of the drafting and enactment of weak, incomplete, unenforced or near-sighted statutes. Unless the various parliaments impose fresh restrictions on the police's authority to obtain and use DNA profiles,[33] it will be the police and those who manage and resource them who will determine the future extent of Australians' behavioural privacy. ●

Jeremy Gans, Faculty of Law, University of Melbourne.

The author's research on DNA sampling is generously funded by the Australian Research Council. Thanks to Kirsten Edwards for comments on a draft.

This article has been peer reviewed.

Endnotes

1. See generally, Gans J and Urbas G 'DNA identification in the criminal justice system' (2002) *Trends & Issues in Crime and Criminal Justice* 226.

2. *Crimes Act 1914* (Cth), Pt ID; *Crimes (Forensic Procedures) Act 2000* (ACT), applicable in Norfolk Island through its *Crimes (Forensic Procedures) Act 2002* (NI); *Crimes (Forensic Procedures) Act 2000* (NSW); *Police Administration Act 1978* (NT), Pt 7 Div 7; *Police Powers & Responsibilities Act 2000* (Qld), Ch 17; *Criminal Law (Forensic Procedures) Act 2007* (SA); *Forensic Procedures Act 2000* (Tas); *Crimes Act 1958* (Vic), Pt 3 Div 30A; *Criminal Investigation (Identifying People) Act 2002* (WA). Except where otherwise indicated, all references to a jurisdiction's legislation are to these respective statutes.

3. Commonwealth, Pt ID Div 4 and s 23XWK; ACT/NI, Pt 2.4 and s 73; NSW, Part 4 and s 70; NT, s 145A (and s 95B of the *Prisons (Correctional Services) Act 1980* (NT)); Queensland, s 481 (suspects only); SA, Pt 2 Divs 2 and 3; Tasmania, Pt 2 Div 3 and Pt 3; Victoria, s 464SA (suspects only); WA, s 44 and Pt 7 (suspects only). In Queensland and WA, mass sampling of prisoners was authorised from 2002 to 2005.

4. NSW Ombudsman *DNA sampling and other forensic procedures conducted on suspects and volunteers under the Crimes (Forensic Procedures) Act 2000* Sydney 2006 pp 100–02.

5. Commonwealth, Pt ID Div 6B; ACT/NI, Pt 2.8; NSW, Pt 8; NT, s 145B; Queensland, Ch 17 Pt 2; SA, Pt 2 Div 1; Tasmania, Pt 4; Victoria, s 464ZGB; WA, Pt 4 Div 2.

6. Commonwealth, Pt ID Div 3 and s 23XWC(1)(a); ACT/NI, Pt 2.3 and s 65(1)(a); NSW, Pt 3 and s 63(1)(a); NT, s 145(2)(a) (suspects only); Tasmania, Pt 2 Div 2 (suspects only); Victoria, s 464R(2)(a) (suspects only); WA, ss 40(1) and 51(1).

7. NSW Ombudsman *The Forensic DNA Sampling of Serious Indictable Offenders Under Part 7 of the Crimes (Forensic Procedures) Act 2000* Sydney 2004 p 93; NSW Ombudsman, above note 4 at p 88.

8. Guthrie cards refer to the blood samples routinely collected from every newborn in Australia since the 1970s to check for diseases such as cystic fibrosis.

9. *R v Truong Hong Phuc & Truong Thi Van* [2000] VSC 242; BC200003329; *R v Daley* [2001] NSWSC 1211; BC2001018822; *R v Nicola* [2002] NSWCCA 63; BC200203043; *R v Kane* (2004) 144 A Crim R 496; *R v White* [2005] NSWSC 60; BC200500424.

10. Commonwealth, ss 23YDAE and 23YO; ACT/NI, ss 96 and 111; NSW, ss 92 and 109; NT, s 147B(1); Queensland, s 489(3); SA, s 45(2); Tasmania, s 53; Victoria, ss 464ZGH and 464ZGK; WA, s 73.

11. Commonwealth, s 23YDAF; ACT/NI, s 97; NSW, ss 83A and 93; NT, s 147B(2) (matches to profiles relating to offences carrying a maximum penalty of less than 14 years of imprisonment only); Queensland, s 494(1)(a) (and s 8I(2) of the *Police Powers and Responsibilities Regulations 2000* (Qld)); SA, s 45(3)(a); Tasmania, s 54; Victoria, s 464ZGI; WA, s 62(1).

12. See Gans J 'DNA identification and rape victims' (2005) 28 *UNSW Law Journal* 272, 277–80.

13. Commonwealth, s 23YDAF; ACT/NI, s 97; NSW, s 93; Queensland, s 494 (and s 8M and Sch 8 of the *Police Powers and Responsibilities Regulation 2000* (Qld)) (comparisons with CrimTrac profiles only); SA, s 45(3)(b) (foreshadowing a regulation limiting matching); Tasmania, s 54; Victoria, s 464ZGI; WA, s 78.

14. Commonwealth, *Crimes Act Amendment (Forensic Procedures) Act (No 1) 2006*, ss 27A–29, Explanatory Memorandum, items 28 and 29; Supplementary Explanatory Memorandum, Amendment 5; Queensland, *Police Powers and Responsibilities (Amendment) Regulation 2004*, s 8; Tasmania, *Forensic Procedures Order 2006*, s 4.

15. *Crimes Act Amendment (Forensic Procedures) Act (No 1) 2006* (Cth), ss 27, 30 and 31.

16. *Crimes Act 1914* (Cth), s 23YUD. Compare with Australian Law Reform Commission *Essentially Yours: The Protection of Human Genetic Information in Australia* Report No 96 (2003) Sydney, rec 40-2.

17. *Criminal Investigations (Identifying People) Act 2002* (WA), s 61 (defining 'forensic database').

18. Commonwealth, Pt 1D Div 8; ACT/NI, Pt 2.10; NSW, Pt 10; NT, s 147C(1) (permitting retention so long as the Commissioner of Police sees fit); Queensland, s 490; SA, *Criminal Law (Forensic Procedures) Act 1998*, Pt 4A, Div 4 (now repealed); Tasmania, Pt 7; Victoria, ss 464ZG and 464ZGE; WA, ss 62(1)(c), 63(1)(c), 64(1)(c), 65(1)(c), 66(2)(c) and 67(1)(c).

19. Commonwealth, ss 23YDAG and 23XY; ACT/NI, ss 98 and 86; NSW, ss 94 and 83; Queensland, ss 530 and 531 (criminal offence only); SA, *Criminal Law (Forensic Procedures) Act 1998*, ss 45(3) and 46C (now repealed); Tasmania, s 55 (criminal offence only); Victoria, ss 464ZG(8)–(9), 464ZGE (9)–(10), 464ZGJ and 464ZE(1)(d); WA, ss 74 and 84.

20. Sections 69 and 70(1) (applicable to all profiles apart from those from non-'involved' volunteers).

21. SA Auditor-General *Supplementary Report: Government Management and the Security Associated with Personal and Sensitive Information* (2005) pp 11–13 and 34–35.

22. *R v Dean* [2006] SADC 54 (25 May 2006).

23. SA Auditor-General *Supplementary Report: Matters Arising from the Further Audit Examination of the Administration of the Criminal Law (Forensic Procedures) Act 1998 and Other Matters* (2006) pp 5–6.

24. SA Legislative Council *Hansard* 2007 p 1437; SA House of Assembly *Hansard* 2007 p 1649.

25. The only destruction requirement is for victims and volunteers, who must request that their DNA profile be destroyed: s 39.

26. *Criminal Justice and Police Act 2001* (UK), s 82, inserting s 64(1A) and (3AC) into the *Police and Criminal Evidence Act 1984* (UK). Compare with *Attorney General's Reference No 3 of 1999* [2000] UKHL 63; [2001] 2 WLR 56 (14 December 2000).

27. Association of Chief Police Officers of England, Wales & Northern Ireland *Exceptional Case Procedures for Removal DNA, Fingerprints and PNC Records* (2006) London, at <www.acpo.gov.uk/policies.asp>.

28. Forensic Science Service 'Fact Sheet No 4: Familial Searching' at <www.forensic.gov.uk/forensic_t/inside/news/documents/Familialsearching.doc>.

29. Smith D 'Secret weapon' *The Sunday Times Magazine* 15 October 2006.

30. Section 147C(3); compare with *Police Administration Regulations 1994* (NT), s 20B(2).

31. Unofficial sources suggest that a familial screening was performed during the high-profile Peter Falconio investigation: Wilton M 'Gunman hunt — police fly to UK' *The Northern Territorian* 14 August 2001; Bowles R *Dead Centre* Bantam, Sydney 2005 p 78.

32. See, for example, the inventor of DNA identification, Sir Alec Jeffreys, who has publicly voiced both views: BBC 'Privacy fears over DNA database' 12 September 2002 at <http://news.bbc.co.uk/2/hi/in_depth/sci_tech/2002/leicester_2002/2252782.stm>.

33. For example, the *Police Administration (Forensic Procedures) Amendment Act 2004* (NT) and *Charter of Human Rights and Responsibilities Act 2006* (Vic) (s 38).

Table 1: Key legislation

Commonwealth	*Crimes Act 1914*
ACT and Norfolk Island* (NI)	*Crimes (Forensic Procedures) Act 2000*
NSW	*Crimes (Forensic Procedures) Act 2000*
NT	*Police Administration Act 1978*
Queensland	*Police Powers and Responsibilities Act 2000*
SA	*Criminal Law (Forensic Procedures) Act 2007*
Tasmania	*Forensic Procedures Act 2000*
Victoria	*Crimes Act 1958*
WA	*Criminal Investigations (Identifying People) Act 2002*

* ACT law applicable in Norfolk Island through the *Crimes (Forensic Procedures) Act 2002* (NI).

Table 2: DNA procedures — key provisions (legislative references are to those in Table 1 unless otherwise noted)

	CTH	ACT/NI	NSW	NT	QLD	SA	TAS	VIC	WA
Compulsory DNA sampling without judicial approval.	Pt ID Div 4 and s 23XWK.	Pt 2.4 and s 73	Pt 4 and s 70	s 145A (and s 95B of the *Prisons (Correctional Services) Act 1980*)	s 481 (suspects only)	Pt 2 Divs 2 and 3	Pt 2 Div 3 and Pt 3	s 464SA (suspects only)	s 44 and Pt 7 (suspects only)
Consensual DNA sampling where no power is available.	Pt ID Div 6B	Pt 2.8	Pt 8	s 145B	Ch 17, Pt 2	Pt 2 Div 1	Pt 4	s 464ZGB	Pt 4 Div 2
Consensual DNA sampling where a power is available.	Pt ID Div 3 and s 23XWC(1)(a)	Pt 2.3 and s 65(1)(a)	s 145(2)(a) (suspects only)	N/A	N/A	N/A	Pt 2 Div 2 (suspects only)	s 464R(2)(a) (suspects only)	ss 40(1) and 51(1)
Use and disclosure of DNA profiles.	ss 23YDAE and 23YO	ss 96 and 111	ss 92 and 109	s 147B(1)	s 489(3)	s 45(2)	s 53	ss 464ZGH and 464ZGK	s 73
Restrictions on matching volunteers' DNA profiles.	s 23YDAF	s 97	ss 83A and 93	s 147B(2) (matches to profiles relating to offences carrying a maximum penalty of less than 14 years' imprisonment only)	s 494(1)(a) (and s 8I(2) of the *Police Powers and Responsibilities Regulations 2000*)	s 45(3)(a)	s 54	s 464ZGI	s 62(1)
Other restrictions on matching DNA profiles.	s 23YDAF	s 97	s 93	N/A	ss 8M and 494 (and Sch 8 of the *Police Powers and Responsibilities Regulations* (comparisons with CrimTrac profiles only))	s 45(3)(b) (foreshadowing a regulation limiting matching)	s 54	s 464ZGI	s 78
Destruction of DNA profiles.	Pt ID Div 8	Pt 2.10	Pt 10	s 147C(1) (permitting retention so long as the Commissioner of Police sees fit)	s 490	N/A	Pt 7	ss 464ZG and 464ZGE	ss 61(1)(c), 63(1)(c), 64(1)(c), 65(1)(c), 66(2)(c) and 67(1)(c)
Enforcement of destruction rules.	ss 23YDAG and 23XY	ss 98 and 86	ss 94 and 83	ss 530 and 531 (criminal offences only)	N/A	N/A	s 55 (criminal offences only)	ss 464ZG(8)–(9), 464ZGE(9)–(10), 464ZGJ and 464ZGE(1)(d)	ss 74 and 84

Something for Kate? Privacy developments in the UK

Tony Wilson
FREEHILLS

In a recent decision[1] in the English Court of Appeal, copies of handwritten journal entries by Prince Charles, which had come into the possession of the *Mail on Sunday* newspaper, were held to be relevantly private. Prince Charles had commenced legal action after substantial extracts from his journals were published.

The decision contains a helpful survey of the English position on the protection of private information following the importation of the European Convention on Human Rights (the Convention) into domestic law in 1998[2] and the subsequent decisions in *Campbell v MGN Ltd*[3] and *Douglas v Hello!*.[4] It clarifies the relationship between what may be protected by the duty of confidentiality and the recently acknowledged tort of the misuse of private information, and the shift of the centre of gravity of the action for breach of confidence following the impact of the human rights Convention's articles.

Prince William's girlfriend Kate Middleton, the latest British celebrity to be harassed by 'gutter press tactics', almost certainly will be a beneficiary of this gravitational shift. The recent upholding of a complaint by Elle McPherson to the Press Complaints Commission[5] about photographs of her and her children while holidaying on the private island of Mustique also reinforces the trend towards the protection of the privacy of public figures or celebrities in circumstances where they have a reasonable expectation of privacy, where photographs taken of them in such circumstances cannot be said to be in the public interest.

Prince Charles' journals

Prince Charles has maintained a written journal describing various activities in his public life over many years. On occasion he authorised the distribution of photocopies of pages from his journal under cover of letters marked 'private and confidential' to a limited number of friends and contacts identified by him. The journals were otherwise kept under lock and key. Apart from their common law duties of fidelity and confidentiality, his staff were bound by express confidentiality clauses in their employment contracts.

Publication

The evidence at trial established that one of Prince Charles' former employees had made extra copies of particular journal entries which made their way through a third party to Associated Newspapers Ltd.

The journal entries in question included a description of a banquet attended on the occasion of the handover of the colony of Hong Kong to the Chinese Government in 1993. The comments were 'disparaging of the formalities and of the behaviour of the Chinese participants'.

Substantial extracts from the photocopies of the journal entries were published by the *Mail on Sunday* on 13 November 2005, some days after a visit to England by the Chinese president during which a banquet was held at the Chinese Embassy, an invitation to which was declined by Prince Charles.

Heads of claim

Prince Charles' action alleged:

- breach of copyright;
- breach of confidence; and
- on the basis of the *Human Rights Act 1998* (UK) and Convention articles imported into English domestic law, interference with his right to respect for his private life and his correspondence.

The newspaper relied on the defences of fair use, the absence of confidentiality in the material published and submitted that publication was justifiable under the Convention's article relating to freedom of expression.

Because the trial judge had allowed an application for summary judgment on behalf of Prince Charles, the newspaper on appeal challenged the trial judge's finding that there were no factual disputes of any substance. The Court of Appeal agreed with the trial judge's decision as to the appropriateness of deciding the summary judgment application and went on to consider whether the trial judge's application of the law produced the correct result in favour of Prince Charles.

> [The decision] clarifies the relationship between what may be protected by the duty of confidentiality and the recently acknowledged tort of the misuse of private information …

Breach of confidence

According to the trial judge, the starting point for consideration of the modern law relating to breach of

confidence in England is the House of Lords' decision in *Campbell v MGN*, which required a balancing exercise involving the two relevant Convention articles.[6] According to the Court of Appeal, that approach was too narrow. In giving effect to the Convention rights, English courts should, as far as possible, develop the common law by giving the *Human Rights Act* 'full, direct, horizontal effect'.[7]

Campbell v MGN is an example of the protection of the Convention right to private and family life under Art 8, in the absence of a breach of a confidential relationship. Other recent cases before English courts involving public figures asserting rights in relation to private activities have also involved no relevant breach of confidentiality. As the Court of Appeal notes, the central issue in these types of cases has been whether the information was of a private nature so that its disclosure interfered with Art 8 rights and involved a consideration of the balance between Arts 8 and 10[8] (freedom of expression).

The position now is that 'the courts have extended the law of confidentiality so as to protect Art 8 rights in circumstances which do not involve a breach of a confidential relationship'.[9] According to the Court of Appeal, a consistent approach to the applicable legal principles was evident in the judgments in *Campbell v MGN* (even though different factual conclusions were drawn), as outlined in the judgment of Lord Nicholls of Birkenhead:

> Now the law imposes a 'duty of confidence' whenever a person receives information he knows or ought to know is fairly and reasonably to be regarded as confidential. Even this formulation is awkward. The continuing use of the phrase 'duty of confidence' and the description of the information as 'confidential' is not altogether comfortable. Information about a person's private life would not, in ordinary usage, be described as 'confidential'. The more natural description today is that the information is private. The essence of the tort is better encapsulated now as misuse of private information.[10]

Where information is confidential and private what is the impact of the Convention's protection for freedom of expression?

In Prince Charles' case, however, there was an enforceable duty of confidentiality arising out of the common law duty between employer and employee and the confidentiality clauses in the contracts of people employed by him. It was noted that the newspaper was aware of these breaches of confidence. But it was this older notion of the protection of confidential information which the newspaper had to overcome by relying on the Conventions' freedom of expression protection.

The court proceeded to consider what is relevantly 'confidential' or 'private'. The journals were, according to the court, 'paradigm examples of confidential documents'.[11] They were

… the central issue in these types of cases has been whether the information was of a private nature so that its disclosure interfered with Art 8 rights and involved a consideration of the balance between Arts 8 and 10 …

also clearly intended to be, and remain, private.

In considering what makes a document 'private', the court looked at three issues.

- Is it the nature of the information?
- Is it the form in which the information is conveyed?
- Is it the fact that the person disclosing the information is in a confidential relationship with the person to whom the information relates?

By the very nature of Prince Charles' journals, the court considered that even if a copy had been inadvertently sent to an unintended recipient or had been 'lost' by an intended recipient 'its form and content would clearly have constituted private information entitled to the protection of Article 8(1) as qualified by Article 8(2)'.[12]

Applying the test from *Campbell v MGN*, Prince Charles had a 'reasonable expectation' that the content of his journals would remain private. None of the newspaper's opposing submissions were successful. The arguments in favour of the journals being in the public domain, or that Prince Charles' alleged relaxed way of dealing with them denied them protection, had no merit. The suggestion that Prince Charles, as next in line to the throne and a public figure who courted public attention through controversy, particularly in relation to matters broadly political, meant that he could have no reasonable expectation that the content of the journals, if disclosed, would remain confidential, was also rejected. The Court of Appeal agreed with the trial judges' view that these matters did not go to the question of the confidentiality of any particular content but to the proportionality test in considering whether material claimed to be confidential must give way to the public interest in freedom of expression.

Private information and freedom of expression

In *Campbell v MGN*, Lord Hoffman, noting a shift in the centre of gravity of the action for breach of confidence when it is used as a remedy for the unjustified publication of personal information referred to 'incremental changes' to the duties arising from a relationship of trust and confidence extending it to a wider group of people.[13] In addition, the new approach alters and expands the underlying values protected by the law in this area. Rather than being based on a duty of good faith, it focuses upon the protection of human autonomy and dignity — the right to control the dissemination of information about one's private life and the right to the esteem and respect of other people.[14]

This new approach is clear in the decision in *Campbell v MGN*. In this case, Naomi Campbell's attendance at Narcotics Anonymous received press attention because there was a breach of confidentiality by a fellow participant or an employee or associate. But as noted by the Court of Appeal, if Campbell herself had not put her drug experiences into the public domain, publishing it would have been an interference with her Art 8 rights.

The court's judgment in the present case, delivered by Lord Phillips of Worth Matravers, continues with a discussion of the importance of the role of the press in a democratic society, and the role and impact of the consideration of the Convention's protection of freedom of expression in these types of cases.

Clearly, English law in relation to privacy has moved forward. Prince Charles would have been entitled to the protection he sought for his journals in the absence of a breach of confidentiality. The fact that there were breaches of confidence by a member of his staff added further weight to his claim.

Something for Kate

There is no doubt that celebrity hunting is big business. English tabloids thrive on it. Even the tragic death of Princess Diana did not abate the public's demand for information, including photographs of celebrities, which are even more desirable when showing private moments of misbehaviour in public.

However, the decision in favour of Prince Charles and some other unrelated events may stem the tide of intrusion and harassment by certain sections of the media. In January 2007, the *News of the World*'s former Royal Editor, Clive Goodman, was jailed for four months for tapping into voicemails left for aides of Princes' Charles, William and Harry, and the private investigator who assisted him to do so was jailed for six months. Complaints to the UK Press Complaints Commission, like that of Elle McPherson, will increase pressure on the editors and publishers of tabloids and celebrity magazines to abandon gutter press strategies.[15]

Kate Middleton's lawyers wrote to the Press Complaints Commission in January this year after making a secret video showing paparazzi photographers harassing her as she left home for work and other private activities. The letter said, in part: 'My client strongly objects to having her photograph taken in a public place while going about her private business'.[16]

The position in Australia

At the 80th birthday celebration of the *Australian Law Journal* in Sydney on 17 March 2007, Justice Michael Kirby said that Australia was out of step with legal practice throughout the developed world by failing to protect the basic rights of citizens with a Bill of Rights. Such a development was inevitable, he added.[17]

The ACT has enacted the *Human Rights Act 2004* and Victoria, *The Charter of Human Rights and Responsibilities Act 2006*. A debate about protecting human rights has been stimulated anew by anti-terrorism legislation which arguably has the potential to seriously abrogate human rights and freedoms.[18] George Williams notes[19] that the Victorian Charter draws largely on similar legislation in the UK and NZ, that it protects the rights of most importance to an open and free democracy, including privacy, and sets out a balancing test based on a number of specified factors.

On 28 March 2007, the WA Government introduced the Information Privacy Bill 2007 (WA). Similar legislation is being considered in NSW.[20]

It appears inevitable in a world in which technology makes personal and private information readily accessible, that legal constraints and barriers to the access and use of such information are increasingly required and demanded. Australia will soon adopt an opt-out regime for unsolicited

telephone marketing.[21] In America, a movement is underway to apply an opt-out scheme to unsolicited printed material by post.

To add to this mix in Australia is the apparent increase in government secrecy reflected in recently published statistics about the success rates for freedom of information requests[22] and the High Court of Australia's recent validation of conclusive certificates in *McKinnon v Secretary, Department of Treasury*.[23]

Postscript

On 3 April, Judge Hampel handed down her decision in *Jane Doe v Australian Broadcasting Corp*.[24] The individual defendants (Terence Rickard and Valerie Veo) were changed, under s 4(1A) of the *Judicial Proceedings Reports Act 1958* (Vic), with publishing information identifying a victim of a sexual offence. After their conviction, the plaintiff commenced proceedings against them and their employer for damages for breach of statutory duty, negligence and breach of privacy. After consideration of the earlier Australian decisions in *Grosse v Purvis*[25] and *Giller v Procopets*,[26] and in the context of the English developments in privacy law, discussed above, her Honour held that the alleged invasion or breach of privacy was an actionable wrong allowing a right to recover damages according to the ordinary principles governing damages in tort. General damages for invasion of privacy, breach of confidence, associated hurt, distress, embarrassment, humiliation, shame and guilt were assessed at $110,000, in addition to special damages for past lost earnings and medical expenses. ●

Tony Wilson, Consultant, Freehills, Perth.

Endnotes

1. *Associated Newspapers Ltd v His Royal Highness the Prince of Wales* [2006] EWCA CIV 1776.
2. *Human Rights Act 1998* (UK).
3. [2004] 2 AC 457.
4. [2006] QB 125.
5. Adjudicated on 29 January 2007. The adjudication is available from the Press Complaints Commission at <www.pcc.org.uk/cases/adjudicated.html>.
6. See, generally, Wilson T 'English Court of Appeal advances protection of private information' (2005) 2(1) *Priv LB* 7.
7. See Morgan J 'Privacy, confidence and horizontal effect: "Hello" trouble' (2003) *CLJ* 444.
8. Article 10 of the Convention concerns the right to freedom of expression, including the right to hold opinions, and to receive and impart information and ideas without interference from a public authority.
9. Above note 1 at [26].
10. Above note 3 at 464 [14].
11. Above notes 1 at [35].
12. Above note 1 at [36].
13. Above note 3 at 473, [51].
14. Above.
15. The last two paragraphs are drawn from Fitzsimmons C 'Gossip hunger fuels gutter press tactics' *The Australian* 5 February 2007 p 32.
16. See Kent P 'Kate issues last warning' *The Sunday Times* 21 January 2007 p 40.
17. 'Bill of Rights inevitable, says Kirby' *The West Australian* 17 March 2007 p 60.
18. See Wynhausen E 'Spies like us: we never walk alone' *The Weekend Australian* 27–28 January 2007 p 27.
19. Williams G 'Lessons from Victoria's Charter of Human Rights and Responsibilities' (February 2007) *Law Society Journal NSW* p 68.
20. See Merritt C 'Privacy law to hit press freedom' *The Australian* 22 March 2007 p 13.
21 Under the *Do Not Call Register Act 2006* (Cth); the Do Not Call Register, to be operated by the Australian Communications and Media Authority, is due to be operational this year. Visit <www.acma.gov.au> for further information and see Cole N and Sainty K 'Do Not Call Register' (2006) 3(3) Priv LB 39 for a discussion of the legislation.
22. See Merritt C 'Pattern of FOI secrecy emerges' *The Australian* 22 March 2007 p 14.
23. (2006) 229 ALR 187.
24. [2007] VCC 281. There will be a more detailed outline and discussion of this decision in the next issue of the *Privacy Law Bulletin*.
25. (2003) Aust Torts Reports ¶81-709.
26. [2004] VSC 113; BC200402552.

Book review

New Dimensions in Privacy Law: International and Comparative Perspectives

Andrew T Kenyon and Megan Richardson (eds)

Cambridge University Press ISBN: 0521860741 Price: $199 (inc GST) November 2006

Reviewed by **Karin Clark** ALLENS ARTHUR ROBINSON

Australian privacy law is 'new' for most Australian legal practitioners. It was only in 2001, when the National Privacy Principles under the *Privacy Act 1988* (Cth) became binding on Australian businesses and the High Court opened the possibility of a new action for invasion of privacy in *Australian Broadcasting Corp v Lenah Game Meats*,[1] that privacy law began to impact on a wide range of practice areas, from workplace relations to finance and banking, IT outsourcing to health law practices, and all commercial practices that advised clients who collected, handled and needed to protect personal data.

In this context, the editors of this collection of essays, Andrew Kenyon and Megan Richardson, have done a valuable service not only to academic lawyers conducting privacy law research but also to privacy law practitioners. Many of us are conscious that a good understanding of both data protection principles and common law trends in privacy protection depends significantly on appreciating the international and comparative frameworks in which these have been developed and continue to change. However, we have not yet had many opportunities to access, in one volume, recent scholarship about these issues.

This book originally grew out of a series of public seminars held about privacy law and policy under the auspices of the Centre for Media and Communications Law at the University of Melbourne in 2003 and 2004. The editors note that the essays originally presented at those seminars were further developed for this collection and further chapters were also commissioned to increase its range. Together, the articles offer research and commentary on interrelated themes that include:

- comparisons of recent general law trends in privacy protection;
- the impact of technological developments on privacy policy and law;
- recent international frameworks that have been developed for the protection of personal data; and
- fresh observations about how concepts such as privacy and freedom of speech interrelate in practice.

It is not possible in a short review to do any justice to the rich and complex contributions in this volume, but the following are some of the essays that may be of particular interest to the Australian practitioner.

… a good understanding of both data protection principles and common law trends in privacy protection depends significantly on appreciating the international and comparative frameworks in which these have been developed and continue to change.

Graham Greenleaf's chapter on the APEC Privacy Framework[2] dissects the most recent transnational instrument for a regional privacy framework, the development of which could ultimately significantly affect how personal data is moved between Australia and its closest neighbours. His analysis shows how the APEC Principles (which are helpfully set out in an appendix to the chapter) fall short of the standards of the OECD Principles (and thus so much more the privacy principles in the EU Directive Guidelines). The chapter concludes that while there is a danger that the lower standards in the APEC Principles will become accepted as a 'ceiling' in Asia–Pacific countries, their acceptance by APEC member countries may (on the other hand) encourage countries that have no systematic information privacy laws at all to implement them. It should be noted that while Professor Greenleaf expresses concern that the 'cross-border elements' in the APEC Framework (which had not been developed at the time that he wrote the chapter) might have the effect of preventing data export restrictions within the APEC region (provided that the Framework's relatively low standards were met), this concern seems to have been obviated with the finalisation of the Framework.[3]

Another chapter that also addresses the international exchange of personal data is by Yves Poullet and J Marc Dinant, about the regulation of privacy in the online environment.[4] Australian lawyers have become conscious that as most transfers of personal information to and from Australia are electronic, international as well as Australian rules regulating the online transfer of personal data are relevant to whether, and under what conditions, such transfers are permitted. The authors of this chapter have been active in the

European debate about the extent to which legal rules and principles on privacy protection should be modified given the exponential growth and increasing invasiveness of new internet applications. Among the issues they discuss, and that will no doubt be debated in Australia in the context of the current Australian Law Reform Commission's review of privacy, are:

- whether the definition of 'personal information' should continue to relate only to identifiable (or reasonably identifiable) individuals or should extend to other global unique identifiers or IP addresses; and
- the extent to which new technologies should give rise to new consumer rights, including users' rights to more complete control of their ICT environment and terminal equipment.

Another fascinating chapter which discusses the regulation of electronic surveillance, but in the context of digital rights management (DRM) technology, is by David Lindsay and Sam Ricketson.[5] This chapter explains the relationship between copyright law and the potential threat to privacy posed by DRM technology, because of (among other things) the potential for the collection of identifying information and the continuing surveillance and monitoring of end users of protected content. Here again, the adequacy of the definition of 'personal information' in the Australian *Privacy Act* is discussed, as well as the principles and interests that should underpin the regulation of surveillance (both covert and overt) using such new technologies.

Three chapters deal with overseas trends in the general law protection of privacy. Megan Richardson and Lesley Hitchens[6] analyse the trends in recent cases that have allowed celebrities greater control over the aspects of their lives that they choose to become public. Interestingly, the authors are able to trace the inclination of the courts to support privacy as a matter of individual choice as far back as the reasoning in the 1849 case of *Prince Albert v Strange*.[7] Gavin Phillipson's comparison of the 'right of privacy'[8] as developed by the House of Lords in *Campbell v MGM Ltd*[9] and the European Court of Human Rights in *Von Hannover v Germany*[10] focuses on the different understandings that these courts have about the meaning of 'private life' and also discusses whether these views can be reconciled. He also argues persuasively that the House of Lords decision has effectively given English law a privacy tort in effect (if not in name). On this point, Raymond Wacks clearly takes a different view in his chapter entitled 'Why there will never be an English common law privacy tort',[11] where he argues that the use of doctrines about breach of confidence are inadequate to protect privacy and highlights different views between the English judges themselves about what constitutes 'private information'. Australian lawyers are likely to find interest in all three chapters since, if the Australian courts do decide to provide litigants with privacy protection, they are likely to need to consider and evaluate the merits of the different approaches that have been taken by overseas courts recently. ●

Karin Clark, Special Counsel, Allens Arthur Robinson.

Endnotes

1. (2001) 185 ALR 1 — however, the promise of an Australian action has not yet eventuated (*Kalaba v Commonwealth* [2004] FCA 763; BC200403700 and *Giller v Procopets* [2004] VSC 113; BC200402552). See, however, the very recent judgment of Hampel J of the Victorian County Court in *Jane Doe v ABC* [2007] VCC 281.
2. 'APEC privacy framework sets a new low standard for the Asia–Pacific' Chapter 5.
3. Greenleaf G 'APEC Privacy Framework completed: no threat to privacy standards' [2006] *PLPR 5*, available at <www.austlii.edu.au/au/journals/PLPR/2006/5.html>.
4. 'The internet and private life in Europe: risks and aspirations' Chapter 4.
5. 'Copyright, privacy and digital rights management (DRM)' Chapter 6.
6. 'Celebrity privacy and benefits of simple history' Chapter 10.
7. (1989) 47 ELR 1302.
8. 'The "right" of privacy in England and Strasbourg compared' Chapter 8.
9. [2004] 2 AC 457.
10. (2005) 40 EHRR 1.
11. Chapter 7.

eye spy PRIVACY NEWS

Australia

Privacy legislation tabled in WA

28 March 2007. The Information Privacy Bill 2007 (WA) was recently introduced into WA Parliament, in what will be the state's first comprehensive legislative package on information privacy.

In general, the Bill proposes to:

- regulate the handling of personal information by the public sector;
- regulate the handling of health information by the public and private sectors;
- create a right to apply for access to, and amendment of, health records by the private sector; and
- facilitate the exchange of health information held by the public sector in appropriate circumstances.

The Bill will:

- establish a set of Information Privacy Principles governing the handling of personal information by the public sector;
- establish a set of Health Privacy Principles governing the handling of health information by the public and private sectors;
- provide for the making and approval of information privacy codes of practice and health privacy codes of practice;
- provide for the making of complaints in respect of alleged interferences with privacy and decisions relating to access to, and amendment of, health records, and establishes processes for the resolution of those complaints;
- establish the Office of Privacy and Information Commissioner to encompass the existing Office of Information Commissioner;
- enable the Offices of Parliamentary Commissioner and Privacy and Information Commissioner to be held concurrently; and
- amend the *Freedom of Information Act 1992* (WA), the *Parliamentary Commissioner Act 1971* (WA) and other Acts as a consequence of the enactments of the *Information Privacy Act 2007* (WA). ●

Source: Explanatory Memorandum to the Bill.

Queensland telecommunications interception Bill tabled

15 March 2007. The Terrorism, Organised Crime and Anti-Corruption Surveillance Bill 2007 (Qld) has been introduced into Queensland Parliament.

According to s 3, the main objective of the Bill is to 'establish a recording, reporting and inspection regime to complement the *Telecommunications (Interception and Access) Act 1979* of the Commonwealth, so that the Queensland Police Service and the Crime and Misconduct Commission may use telecommunications interception as a tool for the investigation of particular serious offences prescribed under the Commonwealth Act'. ●

Access card review continues

15 March 2007. The Senate Standing Committee on Finance and Public Administration has reported back to Parliament following its review of the Human Services (Enhanced Service Delivery) Bill 2007 (Cth), the legislative instrument that will establish the legal framework for the access card.

Among other things, the Committee examined:

- the Bill's provisions relating to the intended scope and purposes of the card;
- the information to be included in the card register, in the chard's chip and on the card's surface; and
- a range of offences prohibiting persons from requiring an access card for identification purposes and prohibiting other improper uses of the card.

The Committee's only agreed recommendation was that the Bill be combined with the proposed second tranche of legislation for the access card into a consolidated Bill. In response to this, the Bill has been removed from Parliament for submission as recommended later this year.

The Committee also identified a number of concerns, which it was unable to address given the limited time for review. These are set out in the Committee's report, available at <www.aph.gov.au/Senate/committee/fapa_ctte/access_card/report/index.htm>.

The Consumer and Privacy Taskforce in the Office of Access Card also recently released a further discussion paper. The discussion paper concerns the registration process for the card. Copies are available at <www.accesscard.gov.au/consumer_privacy_task_force.html>. ●

New national industry standard for telemarketing and research calls

26 March 2007. The Australian Communications and Media Authority (ACMA) has determined a national industry standard for making telemarketing and research calls.

The *Telecommunications (Do Not Call Register) (Telemarketing and Research Calls) Industry Standard 2007* establishes minimum standards intended to provide greater certainty for consumers on the minimum level of conduct they can expect from those making unsolicited telemarketing and research calls.

The industry standard applies to:

- all telemarketing calls made to an Australian number to offer, advertise or promote goods, services, interests in land, business opportunities or investments, or to solicit donations;
- all research calls to conduct opinion polling and to carry out standard questionnaire-based research; and
- calls made for the above purposes by organisations exempt from the general prohibition on calling numbers listed on the Do Not Call Register, such as charities, registered political parties and religious organisations.

A key requirement is to define when calls can and cannot be made.

The industry standard will commence at the same time as Pt 2 of the *Do Not Call Register Act 2006* (Cth), expected to be 31 May 2007. ●

Source: ACMA media release MR 26/2007 (26 March 2007).

Gatekeeper role for ACMA in phone number database scheme

28 March 2007. ACMA will have a 'gatekeeper' role in granting applications for authorisation to use and disclose information from the Integrated Public Number Database (IPND) under a new scheme.

The *Telecommunications Integrated Public Number Database Scheme 2007* has been established as a result of recent amendments to the *Telecommunications Act 1997* (Cth). The IPDN scheme will become operational upon proclamation of the enabling amendments to the *Telecommunications Act*.

'The IPND scheme is intended to ensure that IPND data is only used for authorised purposes and will assist in preventing any misuse of IPND information,' said ACMA Chairman Chris Chapman.

Under the scheme, ACMA will have a gatekeeper role in granting authorisations to use and disclose information from the IPND in connection with the publication and maintenance of a public number directory or for conducting research of a kind specified by the minister.

In addition, IPND scheme imposes conditions upon the granting of authorisations. Conditions include obligations regarding the manner in which corrections are dealt with and the information which must be provided to consumers who are contacted by researchers. ●

Source: ACMA media release MR 32/2007 (28 March 2007).

AUSTRAC rules to assist with AML compliance

30 March 2007. The Australian Transaction Reports and Analysis Centre (AUSTRAC) has finalised a series of rules intended to provide business with greater certainty in complying with anti-money laundering (AML) laws.

The rules set out the requirements with which industry must comply under the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (Cth), including requirements for customer identification and verification procedures, and AML counter-terrorism financial programs. The rules were developed in consulation with industry, the Office of the Federal Privacy Commissioner and the federal Attorney-General's Department.

AUSTRAC CEO Neil Jensen said that, in line with the risk-based approach integral to the legislation, businesses themselves will determine the way in which they meet their obligations.

'The rules fill in a lot of the practical detail of what is required of industry to ensure they comply with the legislation. However, the requirements are risk-based, and reporting entities must design their programs to manage and mitigate their own risks,' said Mr Jensen.

'Importantly, now that these rules are made, it is critical that businesses do not wait until December to put their plans into action. Industry needs to start work now in applying resources to the areas of their operations which they consider put them at greatest risk of exposure to money laundering.'

The legislation comes into effect during a staggered implementation timeframe with the final provisions effective in December 2008. According to AUSTRAC, all of the remaining rules will be finalised before the implementation dates for each relevant section of the legislation. ●

Copies of the rules are available from AUSTRAC at <www.austrac.gov.au>.

International

Don't call me, baby: US FTC reports on registry effectiveness

April 2007. The US Federal Trade Commission (FTC) recently reported to Congress on the effectiveness of the US National Do Not Call Registry. On 11 March 2003, the US Congress passed the *Do Not Call Implementation Act 2003*, which, among other things, implemented the Registry.

The FTC's findings included the following.

- By the end of June 2006, some 132 million telephone numbers were registered.
- In 2005/06, some 6824 entities paid fees totalling US$21,698,970 for access to the National Registry.
- As of 30 September 2006, the FTC had filed 28 cases alleging violations of the National Registry and had reached settlements in 21 of these cases, obtaining injunctive relief in all 21 cases. In 11 of the cases, the court ordered civil penalties totalling more than $7.6 million. In the remaining cases, the court ordered redress and/or disgorgement for other violations, totalling more than $8.2 million. ●

Copies of the report are available at <www.ftc.gov/opa/2007/04/fyi07232.htm>.

PUBLISHING EDITOR: Darren Smith MANAGING EDITOR: Bruce Mills PRODUCTION: Christian Harimanow
SUBSCRIPTION INCLUDES: 10 issues per year plus binder SYDNEY OFFICE: Locked Bag 2222, Chatswood Delivery Centre NSW 2067 Australia
CUSTOMER RELATIONS: 1800 772 772 GENERAL ENQUIRIES: (02) 9422 2222 FACSIMILE: (02) 9422 2404 DX 29590 Chatswood
www.lexisnexis.com.au darren.smith@lexisnexis.com.au

ISSN 1449-8227 Print Post Approved PP 243459/00067

This newsletter may be cited as (2007) 3(9) *Priv LB*