A VERY DYNAMIC ISSUE: INTERNATIONAL DEVELOPMENTS IN PRIVACY IN THE LAST 12 MONTHS

Kimberlee Weatherall*

Paper presented at the ANU Public Law Weekend, Canberra, 2 November 2002

Introduction: International Developments in Privacy, 2002

In 2000-2001 it seemed that we were constantly hearing of some new privacy 'scandal' arising from the collection and use of personal information by the private sector. During this period, we saw the enactment and then in December 2001 the coming into force of the *Privacy Amendment (Private Sector) Act* 2000 (Cth).[1] The year 2000, then, and to a lesser extent 2001 were the years of the private sector privacy debacle.[2] 2002, on the other hand, owing to developments in the wake of the events of September 11, has seen a different focus of concern for privacy advocates. More attention is now given to 'big brother'-like surveillance by law enforcement, and the collection and use of personal information by government. This is because legislatures around the world have sought to give additional powers to law enforcement, for the stated purpose of aiding the 'war against terror'.[3] We might expect that, following the achievement of a long-standing goal of privacy advocates – legislation covering the private sector, however qualified it might be[4] – and in light of the understandable focus on *government* surveillance, developments in relation to privacy in the private sector would be sunk to mere background noise.

Quite the contrary, in fact. For people interested in information privacy law and policy, there have been plenty of international developments to think about since the private sector amendments to the *Privacy Act* came into force in December 2001. Interestingly, too, many of the same issues are cropping up in a number of jurisdictions.

My purpose today is both ambitious, and unambitious. It is ambitious because I aim to highlight some of the recent international developments, to seek to draw some common themes and to identify issues that people concerned about individual privacy (whether companies who have to observe it, or individuals who are worried about its loss) will need to keep an eye on, during the next few years. It is unambitious, because I raise more questions than I can possibly answer. This is an overview paper of the present position. Issues in this area will continue to be as fast-moving into the future as they have been in the last 2 or so years.

Specifically, there are four international developments, occurring in (approximately) the last 12 months, that I want to highlight today. Each has a significant impact on the environment in which private sector entities will be operating when it comes to the collection, use and disclosure of personal information:

* *Lecturer, Faculty of Law, University of Melbourne (formerly Faculty of Law, University of Sydney); Associate Director, Intellectual Property Research Institute of Australia.*

1. Developments in the common law relating to privacy. There have been some important cases handed down particularly in the United Kingdom that address the common law relating to privacy, the most recent on 14 October 2002. Such changes in the 'background' privacy law inevitably has an impact on the way we understand the privacy principles embodied in legislation such as the *Privacy Act* 1988 (Cth);

2. Changing rules whereby private sector entities may be *required* to *retain data*. If enacted, such data retention laws may mean more 'stockpiling' of information by private sector bodies. As we know, once information is stored, people have a tendency to find new uses for it (the phenomenon known as 'data creep').[5] Thus such 'data retention' laws have significant implications for the application of the *National Privacy Principles*.

3. The issue of *access* to data held by private parties – in particular, questions surrounding access sought by *other private parties* seeking to enforce private rights.

4. The need to consider the impact of *other laws* on privacy interests. For example, methods for the enforcement of copyright rights are one area of concern.

The survey below will, I hope, make one thing very clear. There has been a great deal of action internationally in the last year, in ways that impact on the collection and use of personal information and which are not covered by the Privacy Act as amended, or Australian privacy law generally. Developments in the common law relating to breach of confidence in the United Kingdom rely on legislation, specifically the *Human Rights Act* 1998, which has no counterpart in Australia. Orders by law enforcement for data retention by third parties are likely to fall within 'law enforcement exceptions' to the *Privacy Act* and the *National Privacy Principles*.[6] Access to data by private parties would also fall within such exceptions,[7] as would in at least some cases situations where other laws or other interests – such as copyright – impact on privacy rights. In other words, I want to argue that, while there is much to be proud of in the fact that we now *have* private sector privacy legislation, there is going to be a lot of debate in areas at the edges of that legislation, or that fall into gaps in its coverage. I want to sound this warning loud and clear, particularly in light of the need for future review of the legislation.[8] And I wish to make a plea that we constantly monitor the protection of privacy interests, or intrusion on privacy interests, *outside* the remit of the legislation. In an area where developments in technology constantly move the goal posts, to be complacent now we have legislation would be foolish, to say the least. Developments in the last 12 months indicate some areas we should monitor.

Of course, in considering these specific issues and concerns, we should not lose sight of the 'bigger picture' of privacy protection. The reality today in our highly networked, information-intensive society remains one of erosion of information privacy. The basic issues have not changed just because private sector legislation has been enacted, here and overseas. While Privacy Commissioners worldwide work hard to inculcate a 'culture of privacy',[9] they are working against some strong factors that push in an opposite direction. As database and data mining technology become more sophisticated and less expensive, companies increasingly have the capacity to gather large and detailed 'dossiers' on their customers.[10] In an environment where 'information is money', and power, the incentives for such collection are strong.[11] Furthermore, new technologies only strengthen the trend towards collecting ever more detailed, and personal information.[12]

We have some reasons to be (cautiously) optimistic. Privacy legislation contains principles which, when applied, can counter this trend. Principles such as NPP 1.1, which prevents an entity collecting information unless it is 'necessary' for one of the entity's functions,[13] and, in Australia at least, the NPP 8[14] which provides that individuals must, if practicable, have the option of transacting anonymously, hopefully discourage some of this large-scale collecting. Our own Privacy Commissioner has generated an amazing amount of guidance and

information for the private sector in a relatively short time. Elsewhere around the world, other Privacy Commissioners are putting their decisions and recommendations in particular (de-identified) cases online: aside from the Australian site,[15] the Canadian Privacy Commissioner's site,[16] and the equivalent New Zealand site,[17] are worth mentioning specifically. Looking at those decisions, there is reason to be optimistic that at least in some areas, the system is working. These decisions also should reassure us that similar general principles are being accepted in other countries. But the trend towards collection and use of personal information is strong. Regardless of how we handle the particular issues that I wish to highlight today, vigilance in countering these trends is always going to be necessary if we are to provide meaningful protection for the privacy of individuals.

But my focus today is different: it is on some of the 'new' or 'edges' issues that are rising to prominence internationally.

The Common Law of Privacy: Developments in the United Kingdom

2002 has seen a number of cases handed down in the United Kingdom which deal with claims by individuals for infringements of what might be broadly designated as their 'information privacy interests'[18] – by which I mean the interests of the individual in preventing disclosure or other use of information about themselves. The legal basis on which the claims are put in the cases has varied, the most common claim being one for breach of confidence.

What has this to do, one might ask, with information privacy as conceived under legislation like the *Privacy Act* 1988 (Cth)? Surely these areas of law are conceptually different?[19] There are three points to make about this line of authority. First, while only one of these cases required the court to consider an independent claim for damages arising from the UK's *Data Protection Act* 1998,[20] the Act and the EU Data Protection Directive[21] which the Act stems from rate frequent mention in cases where some interference with privacy is being asserted. As a result, we are seeing the development of judicial understandings of terms in that Act which may be worth looking at when issues arise under the Australian legislation. The English legislation is differently worded, and owes its expression to a large extent to the EU Data Protection Directive, but some terms and ideas are common or at least similar.

Second, developments in the common law in relation to privacy interests are an important background to the requirements under data protection legislation such as the *Privacy Act* 1988 (Cth). The *National Privacy Principles* are stated very broadly, and need to be read against a background of what people in a society consider is appropriate conduct in relation to personal information. Case law even in relation to common law actions contributes to the development of this understanding.

Finally, the *Privacy Act* does not supplant general law obligations of confidence.[22] Private entities, particularly those collecting sensitive information, need to be aware of both sets of obligations.

***Protecting Privacy in England through the Action for Breach of Confidence*[23]**

When we look at the English case law, what we see is a line of authority whereby the traditional action for breach of confidence is being expanded to cover more and more 'privacy' interests.[24] The Court of Appeal has noted: [25]

> an increase in the number of actions in which injunctions are being sought to protect the claimants from the publication of articles in newspapers on the grounds that the articles contain confidential information concerning the claimants, the publication of which, it is alleged, would infringe their privacy.[26]

The action for breach of confidence, the Court suggests, *can* extend to protect 'private interests'.[27]

In *A v B & C*,[28] a decision of the United Kingdom Court of Appeal handed down in March 2002, an English premier division footballer sought an injunction to prevent a national newspaper publishing stories about his two extra-marital affairs. A's claim was framed as a claim for breach of confidence. The Court of Appeal overturned the injunction which had been granted by the judge at first instance.[29] It found that the 'relationship' between A, and the two women C and D with whom he had an affair, was 'not [of a kind] which the court should be astute to protect when the other parties to the relationships do not want them to remain confidential'[30] – as compared to a marital relationship, the confidentiality of which a court would protect.[31] It is notable that the decision in the case reflects a conservative morality, while advocating a very liberal attitude towards the press – affirming that courts are not 'censors or arbiters of taste', and that '[w]hether the publication will be attractive or unattractive should not affect the result'.[32] The case is also notable for the effort by the Court of Appeal to provide guidelines for trial judges confronted with such actions where breach of confidence is made the cause of action in a case where privacy interests are sought to be protected.

Most recently, the Court of Appeal handed down its decision in *Naomi Campbell v MGN Ltd*. The act complained of was the publication, by the Mirror, of an article that disclosed that international model Naomi Campbell was a drug addict, and receiving therapy through Narcotics Anonymous. The article included a photograph taken of Ms Campbell leaving (or arriving at) a NA meeting. The case represents the most recent treatment of privacy by the Court of Appeal, and the first which considers the *Data Protection Act* in detail. However, complicating the case were some key concessions by counsel for Ms Campbell. Ms Campbell had claimed in the press that she had not taken drugs. It was therefore conceded that the media could correct that deception. What was complained of, therefore, was the publication of the additional information (in the form of the photograph, and the fact that Ms Campbell was receiving treatment through NA). The breach of confidence claim failed on appeal, the court taking the view that the additional details were a 'legitimate, if not essential, part of the journalistic package' designed to demonstrate that Ms Campbell had misled the public in claiming not to be a drug addict.[33] In identifying when privacy will be protected, therefore, the case itself will be of little assistance owing to its unusual facts.

Campbell v MGN is a particularly interesting case, because claims were *also* made under s 13 of the *Data Protection Act* 1998. It is the first Court of Appeal case that has had to consider, in detail, a claim under the *Data Protection Act*. I argued above that international developments highlight the importance of some of the gaps in Australia's privacy legislation. Note that such a claim could not even have been brought in Australia, owing to the broad exemption under s7B(4) for acts done 'in the course of journalism' (even aside from the absence, under Australian law, of such a private right of action – the point is, complaint could not even be made to our Privacy Commissioner). The *Data Protection Act* claim failed, however, because the actions by the media fell within the UK media exemption.[34]

In these (and other similar) cases the United Kingdom courts have examined in some detail the values which a right of privacy seeks to protect, and the kind of information which may be considered sufficiently 'private' to be worth protecting. As these cases frequently concern celebrities asserting a right of privacy, the courts have also had to engage in an explicit balancing of privacy interests against interests in freedom of expression (a balancing required, of course, by the *Human Rights Act* 1998 (UK)). The decisions are a not insignificant contribution to the international jurisprudence on privacy.

However, a note of caution is necessary in looking to any of these decisions for guidance in Australia. The rapid expansion of the action for breach of confidence, and of privacy law in

general in the United Kingdom, owes much to the enactment of the *Human Rights Act* 1998 (UK). That Act requires a court to act 'in a way which is not incompatible with a [European] Convention [on Human Rights and Fundamental Freedoms] right'.[35] As a result, a court must not act in a way incompatible with Article 8 of the Convention, which mandates 'respect for [a person's] private and family life, his home and his correspondence.' As the Court of Appeal noted in *A v B & C*:

> These [Convention] articles [ie Art 10 and Art 8] have provided new parameters within which the court will decide, in an action for breach of confidence, whether a person is entitled to have his privacy protected by the court … The court, as a public authority, is required not to act 'in a way which is incompatible with a Convention right'. The court is able to achieve this by absorbing the rights which articles 8 and 10 protect into the long-established action for breach of confidence. This involves giving new strength and breadth to the action so that it accommodates the requirements of those articles.[36]

Australia, on the other hand, has no *Human Rights Act* or equivalent constitutional provision. While there are some very tentative suggestions in *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*[37] that common law protection of privacy is not entirely barred by existing case law,[38] there is no support for following the very broad approach being adopted by the United Kingdom Courts – at least just yet.

The Second Development: Data Retention Requirements by Private Parties, and Law Enforcement Access to Privately-Held Data[39]

At the outset of this paper I referred to privacy advocates' focus in 2002 on concerns relating to *government* surveillance and government collection of personal information. As I noted, this focus has been made necessary by legislative developments all over the world which have sought to give additional powers to law enforcement agencies, to counter the 'new' threats from terrorism. Advocates have been concerned to ensure proper safeguards on such law enforcement powers.

This sudden spurt of legislative action to shore up or increase law enforcement powers has not left the data collection practices of the private sector untouched. Quite the contrary. There have been several high profile, and controversial moves to require private parties who are in possession of certain kinds of information to retain that information for a certain period of time – either generally**,** or, at least, on law enforcement entities obtaining an order for retention. The obvious targets for such requirements are telecommunications providers, who have the potential to retain and supply very detailed information which could be very helpful to investigations. Airlines, too, have been a target for such suggestions.

The first of these developments is in the *Council of Europe Convention on Cybercrime.*[40] This Convention was signed in December 2001, and contains provisions which seek to harmonise *substantive* law, but also considerable *procedural* provisions to supplement the powers of law enforcement, and to facilitate assistance between law enforcement entities in signatory countries. In particular, Article 16 of the Convention requires a signatory country 'to enable its competent authorities to order and similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system...', and requires each country to have legislation to oblige a person 'to preserve and maintain the integrity of that computer data for a period of time as long as necessary, up to a maximum of ninety days, to enable the competent authorities to seek its disclosure.'

More recently, in July of this year, the European Parliament agreed to a new Directive on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector.[41] The Directive contains some important privacy protections,[42] but privacy advocates have drawn particular attention to Article 15, which provides that:

> Member States may, *inter alia*, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid out in this paragraph [that is, to safeguard national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorized use of the electronic communication system.]

Note that it is left to each country to determine whether to introduce such laws.[43] This issue has been a particular source of controversy in the United Kingdom, where internet service providers rejected efforts by the Home Office to convince them to subscribe to a Code of Practice whereby they would voluntarily retain such data.[44] It is not clear, at this stage, whether the Minister will choose to use his reserve powers under the legislation to compel ISPs to comply.[45]

There has been controversy too in Canada, where similar provisions for the retention of data by ISPs have been proposed in order to bring Canada into line with obligations it could incur if it signs the *Cybercrime Convention.*[46] Another development in Canada has been a recent proposal by the Canadian Customs and Revenue Agency to retain passenger information on every traveller entering Canada, obtained from airlines, for 6 years. In this case, it would be the government agency actually retaining the information, albeit information obtained from a private party. The proposal has met strong protest from Canada's Privacy Commissioners.[47]

The sheer number of examples where data retention requirements are being discussed, or sought by governments, shows that these are not isolated incidents – but indicative of a trend (how long the trend will last, or how much it will be opposed by members of the public, is another question).

It is worth noting that there are no such explicit requirements for information retention here in Australia,[48] either in relation to telecommunications data, or in relation to airline information,[49] although such requirements have been proposed by the Australian Communications Authority in the past.[50] At present, ISPs in Australia have obligations to provide 'reasonably necessary' assistance to law enforcement agencies,[51] subject to certain limitations, for example the requirement of an interception warrant if the *content* of communications passing over communications networks is to be revealed.[52] History indicates a high level of cooperation with government agencies,[53] and indeed the Privacy Commissioner here in Australia has noted that:

> the Privacy Act is not intended to deter organisations from lawfully cooperating with agencies performing law enforcement functions. Police and other enforcement bodies are generally reliant on the *voluntary* cooperation or organisations to provide information.[54]

Retention of data, particularly wholesale retention of data where no particular offence or suspicion justifies the retention, raises distinct, and troubling privacy issues. Information, once stored, has a tendency to be used for other purposes: we can imagine that if data is retained ISPs can expect more requests for information. There are also objections in principle to allowing government to build databases, using personal information obtained from (or retained by!) third parties, without the individuals' consent, and for purposes not of preventing any particular crime or providing any service, but rather for the sake of having the information available for *potential* use, in case the need comes up. As a result, this is a disturbing trend, that warrants (no pun intended) watching (no pun intended).

The Third Development: Access to Data Held by Private Parties

The third international development that is worth noting is increasing disputes over access by *private parties* to information held by *other* private parties, for the purpose of enforcing

private rights. These disputes are exemplified by the increasing frequency of 'John Doe' suits in the United States, where internet service providers are asked for information identifying individuals who have posted allegedly defamatory comments online.

The first point to note here is that, clearly, access to information held by others for the purposes of enforcing private rights has a very long history: this is what third party subpoenas have always been about in the context of existing legal proceedings.[55] And the common law has long recognised that a private party can seek information from a third party even prior to legal proceedings being brought, for the purpose of identifying potential defendants.[56] Note that, in each case, *some* proceedings must be filed before the order can be made against the innocent third party requiring them to provide the information.

It is predictable that the more information is collected and stored by a private party (and, as noted above, more and more information *is* being held by private parties), the more likely they are to be the target of such requests. Furthermore, because so many transactions online can occur with apparent anonymity,[57] it is becoming more common for potential plaintiffs to seek identifying information from intermediaries – particularly telecommunications carriers and even more particularly, from ISPs. Under most legislative privacy regimes, if a party A (who we assume is bound by the legislation) is holding information and simply receives an *informal request* from wronged party B for the identity of a third party wrongdoer, A may breach the privacy rules if they comply with that informal request.[58] This is something that private entities bound by privacy legislation will need to be very aware of. If, however, a court order or subpoena is obtained by B, then compliance by A will not be a breach – it will be covered by exceptions.[59]

Now, the obvious question is – why should we care whether wrongdoers can be identified? Why have I highlighted this as an 'issue to watch' in relation to privacy and the private sector?

First, there are issues of *process* which, in my view, need to be borne in mind and which, I would argue, should be monitored on an ongoing basis by Privacy Commissioners, and privacy advocates. Subpoenas are frequently issued without a judge first approving it; a judge will look at a subpoena usually only if it is challenged. *Norwich Pharmacal* proceedings are generally held in the absence of the alleged wrongdoer. An innocent third party has little incentive to challenge either subpoenas or *Norwich Pharmacal* orders – their interest, usually, is to get out of the proceedings as soon as possible. In my view, therefore, it is important that the individual alleged wrongdoer have a chance to make submissions or to forward submissions through the party subpoenaed. ISPs or others in receipt of such orders should be required to make reasonable efforts to inform the individual. It is not clear that current law provides an assurance of this procedure. The United Kingdom Court of Appeal has, however, held that it is a desirable procedure to follow: *Totalise Plc v The Motley Fool Ltd, Interactive Investor Ltd.*[60]

Second, there are issues of *scale***.** If significant numbers of such orders or subpoenas are sought, individuals are likely to feel that they are, in fact, living in a 'big brother' state – but where the enforcer is not the State (subject to democratic control) but private parties with private interests – such as copyright owners. ISPs and other data holders, on the other hand, are likely to resent the increase in calls on their resources.[61] Such developments need to be monitored closely.

Third, we need to monitor further developments in legislation, for example, in the copyright area. A dramatic example of the issues is provided by the current *Verizon* dispute in the United States. The Recording Industry Association of America (RIAA) has brought suit against the ISP Verizon.[62] In that suit, the RIAA is seeking to use provisions of the United States Copyright Law[63] to obtain access to information about a Verizon subscriber who is

alleged to be an egregious copyright infringer. If the RIAA is successful, it will mean that, in the United States, an ISP will be required to provide information on user identity even in the absence of *any* proceedings being filed. This means, in effect, there would be no court oversight at all. Legislation which would allow such a result should not be encouraged, and should be challenged – or at least scrutinised very closely if proposed. As noted above, such issues are not going to arise as breaches of the *Privacy Act* 1988 – as exceptions will apply. Rather, this is another area which Privacy Commissioners are well placed to consider part of their general remit, if developments on the ground warrant concern.

The Fourth International Development: The Impact of Other Interests

The final issue I want to highlight, very briefly, is the growing impact of other laws and other interests on information privacy. I am thinking in particular here of the impact that copyright law may have on privacy interests.[64] Copyright owners are increasingly relying on technology to protect their interests in copyright work. In particular, systems for 'digital rights management' are being developed which have the potential to allow copyright owners to monitor, and even bill for, each individual use or access to of a copyright work. This was not possible in an analogue world but is increasingly possible with digital works. Thus I might 'access' a movie online, and be charged each time I viewed it, with a slightly higher charge, perhaps, if I wanted to pause or review elements of it. Such systems clearly have the potential to amass large databases of information on individuals' reading and viewing habits.

Generally accepted Fair Information Practices, and the Australian *National Privacy Principles*, prohibit 'unnecessary' collection, and collection of information in an unfair, or unreasonably intrusive way.[65] But would such collection be 'unreasonable', if done to protect copyright rights and to ensure that each use was remunerated? Copyright owners would probably argue that such a system would allow them to charge much less to people who wanted only to access a work once – thus benefiting people who would not, otherwise, be able to access expensive intellectual works. It is doubtful whether such activities would be affected by NPP 8, which requires the provision of anonymous transacting 'where practicable' – it would be relatively simple to argue that any anonymous system was not 'practicable'. Furthermore, the *National Privacy Principles* clearly allow use or disclosure of information where the individual has 'consented' (as they might have to, in order to obtain access to a copyright work) (NPP 2.1(b)), or if the secondary purpose is 'related' to the primary purpose of collection, and the individual 'would reasonably expect' the organisation to use or disclose the information.

The response to this issue has so far been quite disappointing. The European Union Directive on Copyright in the Information Society recognises the issue but satisfies itself with an exhortation stating that privacy protections 'should' be incorporated into digital rights management systems.[66] United States legislation allows users to 'circumvent' technological measures in order to protect their own privacy, but that exception is extremely limited, and in any event would be available only to those with the skill to do the work themselves.[67] And in Australia, the issue was only very briefly touched on, without offering any firm conclusions, by the *Copyright Law Review Committee* in its recent report *Copyright and Contract*.[68]

Conclusions

No doubt, I have raised far more questions than I can possibly answer. Hopefully, I have provided at least an overview of some of the issues that are arising in the international sphere which have implications for the protection of privacy in relation to the private sector here in Australia. There have been important developments in the common law in relation to privacy in the United Kingdom. And a number of other issues at the edge of current Privacy legislation should, I hope, convince you that there is action at those edges, as well as action in the centre.

Endnotes

1 Subject to the grace period allowed to some small businesses.

2 Dixon, Tim, '2000: A Chronology of Privacy Debacles' (2001) 3(9) *Internet Law Bulletin* 117 (outlining such debacles as the proposed merger of the DoubleClick database with offline material identifying individuals; the proposed sale of a database of personal information on children by Toysmart, and others).

3 In Australia, a raft of legislation concerned with the powers of law enforcement was introduced into Parliament on 13 March, 2002, and subsequently referred to the Senate Legal and Constitutional Legislation Committee on 20 March 2002. The Senate Committee issued its report on 20 May 2002: *Inquiry into the Security Legislation Amendment (Terrorism) Bill 2002 [No.2] and Related Bills* (report available at http://www.aph.gov.au/senate/committee/ legcon_ctte/terrorism/report/Security.pdf (last visited October 28, 2002)). On June 27 2002, the Senate rejected the bill dealing with interception of communications passing over telecommunications systems (*Telecommunications Interception Legislation Amendment Bill* 2002 (Cth)), suggesting that it would unnecessarily extend government surveillance powers: Yeng, Than, 'An ISP's responsibility for co-operating with government agencies in Australia' (2002) 5(2) *Internet Law Bulletin* 13, 19. For a general overview of the developments internationally (including, for example, the US's infamous 'PATRIOT' Act, see Electronic Privacy Information Center (EPIC) and Privacy International, *Privacy and Human Rights 2002: An International Survey of Privacy Laws and Developments* (2002) at 24 (available at http://www.privacyinternational.org/survey/phr2002/) (last visited October 10, 2002)

4 See for example the frequent criticisms of Graham Greenleaf: eg Greenleaf, ''Tabula Rasa': ten reasons why Australian privacy law does not exist' (2001) 24 *UNSWL Jo* 262; Greenleaf, 'Private sector Privacy Act passed (at last).' (2000) 7(7) *Privacy Law and Policy Reporter* 125. Note also the criticisms of the Australian law made by the European Commission's Article 29 Working Party: Hughes, Aneurin, *A Question of Adequacy? The European Union's Approach to Assessing the Privacy Amendment (Private Sector) Act 2000 (Cth)* (2001) 24 *UNSWL Jo* 270.

5 Joel Reidenberg, *Resolving Conflicting International Data Privacy Rules in Cyberspace*, 52 *Stan L Rev* 1315, 1324 (2000); Simson Garfinkel, DATABASE NATION: THE DEATH OF PRIVACY IN THE TWENTY-FIRST CENTURY (2000) at 75 ('Once the day-to-day events of our lives are systematically captured in a machine-readable format, this information takes on a life of its own. It finds new uses. It becomes indispensable in business operations.'); see also Electronic Privacy Information Center (EPIC) and Privacy International, *Privacy and Human Rights 2002: An International Survey of Privacy Laws and Developments* (2002) at 24 (available at http://www.privacyinternational.org/ survey/phr2002/) (last visited October 10, 2002) (noting the problem of 'purpose creep', where 'data collected for one purpose is used for another').

6 *Privacy Act* 1988 (Cth), Schedule 3 (*National Privacy Principles*) (hereafter 'NPPs'), NPP 2.1(f), 2.1(g) and 2.1(h).

7 Esp NPP 2.1(g) (where use of disclosure is 'required or authorised by law').

8 There are areas even aside from those I have mentioned which highlight gaps (or broad exemptions) in our legislation. For example, the Privacy Commissioner of Canada has issued comments on a case where related companies were sharing information – which emphasised the need to make sure customers appreciate potential sharing between related companies: see Privacy Commissioner of Canada: *Alleged Disclosure of personal information without consent for secondary marketing by two telecommunications companies* (16 October 2002), available at http://www.privcom.gc.ca/cf-dc/cf-dc_021016_5_e.asp (last visited 28 October 2002). Our exemption in this scenario is fairly broad: *Privacy Act* 1988 (Cth) s13B.

9 See Office of the Federal Privacy Commissioner, *Information Sheet 13-2001: The Privacy Commissioner's Approach to Promoting Compliance with the Privacy Act* (available at www.privacy.gov.au, last visited 28 October 2002).

10 Daniel Solove has chronicled the rise of database technology in some detail: 'Privacy and Power: Computer Databases and Metaphors for Information Privacy' (2001) 53 *Stan L Rev* 1393

11 See generally Cohen, Julie, 'Privacy, Ideology, and Technology: A Response to Jeffrey Rosen' (2001) 89 *Georgetown L Jo* 2029.

12 For example, privacy advocates have recently raised concerns regarding the wireless Internet and the use of technologies using the Global Positioning System, that allow pinpointing of an individual user's geographical position (raising new possibilities for the collection of behavioural data): see *Something to Watch Over You,* The Economist, 15 August 2002 (available to subscribers at http://www.economist.com/displayStory.cfm?Story_ID=1280634) (last visited 28 October 2002). Digital television, and the possibilities for collecting detailed information about customers' viewing habits, also raises significant privacy issues: David Martin, *TiVo's Data Collection and Privacy Practices*, Privacy Watch Report, Privacy Foundation, March 26, 2001 (http://www.privacyfoundation.org/privacywatch/ report.asp?id=62&action=0) (last visited 28 October, 2002); see also EPIC and Privacy International, *Privacy and Human Rights 2002* (above n5, at 74ff – discussing interactive television). The latest development I have noticed is the implantable human ID chip, the 'VeriChip' – a product of Applied Digital Solutions. ADS has launched a campaign in the United States to promote the device, offering discounts to the first 100,000 people who register to get embedded with the microchip: *Implantable Chip, On Sale Now,* Wired News, 25 October 2002 (available at http://www.wired.com/news/print/0,1294,55999,00.html) (last visited 28 October, 2002). Further issues surround the development of 'ENUM', a technology that aims to

have one contact number for multiple means of communication (email, internet, telephone, mobile): see *Privacy and Human Rights,* above n 5, pp66ff.

13 NPPs, above n 6, NPP 1.1

14 *Id.*

15 http://www.privacy.gov.au

16 http://www.privcom.gc.ca/index_e.asp

17 http://www.privacy.org.nz/top.html

18 'Privacy' as such tends to be applied to a large number of quite different situations. I am concentrating here on *information* privacy – the subject of legislative regimes such as the *Privacy Act* 1988 (Cth) which are concerned with the collection, use and disclosure of personal information, and the access and correction rights of information subjects: Jerry Kang, *Information Privacy in Cyberspace Transactions*, (1998) 50 *Stan L Rev* 1193, 1202-06. Kang distinguishes two other forms of privacy (1) *decisional* privacy: the individual's ability to make decisions without interference, and (2) *spatial* privacy – those principles which shield the individual's 'territorial solitude' from invasion by government (through for example searches), and from private invasion by the law of tort (eg trespass).

19 *R on the application of Ann S v Plymouth City Council* [2002] EWCA Civ 388, para 33 ('The common law obligation to keep a confidence is conceptually quite different from the statutory obligation to process data in accordance with the data protection principles and from the right to respect for private life enshrined in Article 8(1) of the European Convention on Human Rights, although there are overlaps.').

20 *Naomi Campbell v MGN Ltd* [2002] EWCA Civ 1373 (Phillips MR, Chadwick and Keene LJJ, 14 October 2002; [2003] 1 All ER 224). The claim for under the Act was unsuccessful. Under s13 of the *Data Protection Act* 1998, an individual has a private right of action if they suffer damage as a result of a failure to comply with the requirements of the legislation; see also Article 22 of the *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, O.J. L 281, 23/11/1995 p. 0031 – 0050 (hereafter the 'EU Data Protection Directive').

21 Above n 20.

22 *Privacy Act* 1988 (Cth), ss 90, 91

23 *See generally* Singh, Rabinder and Strachan, James, 'The Right to Privacy in English Law' [2002] 2 *European Human Rights L Rev* 129; see also *Privacy Law and Policy Reporter,* volume 8(7) (several articles dealing with the common law 'right' of privacy).

24 *Naomi Campbell v MGN Ltd* [2002] EWCA Civ 1373 (Phillips MR, Chadwick and Keene LJJ, 14 October 2002; [2003] 1 All ER 224); *Campbell v Frisbee* [2002] EWCA Civ 1374 (Phillips MR, Chadwick and Keene LJJ, 14 October 2002); *A v B & C* [2002] 2 All ER 545, [2002] 3 WLR 542 (Lord Woolf CJ, Laws and Dyson LJJ, 11 March 2002). An earlier case that informs this line of caselaw is *Douglas v Hello! Ltd* [2001] QB 967; [2001] 2 All ER 289 (Court of Appeal, Brooke, Sedley and Keene LJJ, 21 December 2000).

25 *A v B & C*, above, n 24, para 3.

26 Ibid.

27 Ibid, para 11(vii)

28 [2002] 2 All ER 545, [2002] 3 WLR 542 (Lord Woolf CJ, Laws and Dyson LJJ, 11 March 2002).

29 *A v B Plc* [2002] E.M.L.R. 7 (Queens Bench Division, Jack J, 10 September 2001).

30 Above n 20, para 44.

31 *Id* para 43.

32 *Id,* para 12(xiii).

33 Above n 24, para 62.

34 *Data Protection Act,* s 32.

35 *Human Rights Act* 1998 (UK), s 6

36 *A v B & C* [2002] 2 All ER 545, para 4

37 (2001) 185 ALR 1

38 See Greenleaf, Graham, 'Privacy at Common Law – Not Quite a Dead Possum' (2002) 8(7) *Privacy Law and Policy Reporter* 129; Stewart, Daniel 'Protecting privacy, property, and possums: *Australian Broadcasting Corporation v Lenah Game Meats Pty Ltd*' (2002) 30 *Fed L Rev* 177.

39 Note: the Electronic Privacy Information Center (EPIC) maintains a website with links to documents on this issue: http://www.epic.org/privacy/intl/data_retention.html (last visited 28 October, 2002).

40 Council of Europe, *Convention on Cybercrime*, 23.XI.2001, available at http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185 (last visited 28 October 2002).

41 *Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector*, OJ L 201/37, 31/7/02.

42 See for example Article 6.1, Article 12 (dealing with directories of subscribers), and Article 13 which deals with unsolicited communications.

43 Such laws are already in place in the UK, the Netherlands, France, Spain and Belgium; similar authority exists in New Zealand: EPIC and Privacy International, *Privacy and Human Rights 2002,* above n5.

44 Millar, Stewart, *Internet Service Providers Say No to Blunkett,* The Guardian, 22 October 2002 (available at http://www.guardian.co.uk/internetnews/story/0,7369,816523,00.html (last visited 22 October 2002).

45 *Id.*

46 Geist, Michael, *Federal Proposal Tells Only Part of the Cybercrime Story,* The Globe and Mail, 3 October 2002, available at http://www.theglobeandmail.com/servlet/ArticleNews/printarticle/gam/20021003/TWGEIS (last visited 10 October 2002).

47 See Canadian Privacy Commissioner, 'Letter from the Privacy Commissioner to the Honourable Elinor Caplan, Minister of National Revenue, about CCRA's plans to establish a massive 'Big Brother' database on the foreign travel activities of all law-abiding Canadians', 26 September 2002 (available at http://www.privcom.gc.ca/media/nr-c/02_05_b_020926_e.asp (last visited 28 October 2002). Similar issues have arisen in the United States: see EPIC's information page on the issue: http://www.epic.org/privacy/airtravel/ (last visited 28 October 2002).

48 In relation to Airline information, Customs here in Australia obtains advance passenger information, but such information is not retained: *Inquiry into the Security Legislation Amendment (Terrorism) Bill 2002 [No.2] and Related Bills,* above n 3, para. 4.68 and following. Note also that in Canada, Customs were last year given the power to obtain such information on undertakings not to retain the information; the proposal to *retain* the information is new.

49 For more detail, see Yeng, above n 3, at 19.

50 Australian Communications Authority, *Record Keeping Rules – Discussion Paper*, available at http://www.aca.gov.au/consumer/discussion/recordkeeprules_dp.pdf) (proposing a 2 year retention rule for certain 'core' data).

51 See *Telecommunications Act* 1997 s 313(3), and s 282(6)

52 *Telecommunications (Interception) Act* 1979 (Cth)

53 Yeng, above n 3, at 13.

54 Office of the Federal Privacy Commissioner, *Information Sheet 7 – 2001 Unlawful Activity and Law Enforcement.*

55 *Supreme Court Rules,*1970 (NSW), Rule 37.2

56 Such orders are known as *Norwich Pharmacal* orders at common law, after the case in which they were first recognised: *Norwich Pharmacal Co v Commissioners of Customs & Excise* [1974] AC 133. They are now embodied in most court rules, including the *Supreme Court Rules* 1970 (NSW) , Section 3.1.

57 By 'apparent' in this context I mean that in fact, the individuals are frequently, although not always identifiable via information such as unique IP addresses. To the 'observer', however, without the information that links the IP address of a user to a name and address of a person, the transactions online, including communications, will frequently be anonymous if the user chooses not to use a name, or to use a pseudonym.

58 But see NPPs (above n 6), NPP2.1(f), and the Internet Industry Association of Australia's *Draft Privacy Code* Version 1.0 (August 2001), available at http://www.iia.net.au/privacycode.html), which provides that the Code Subscriber may disclose if they have 'reason to suspect that unlawful activity has been, or is being or may be engaged in, and uses or discloses the Personal Information as a necessary part of its investigation of the matter…' (Provision 6.8(f)) (the provisions are in the same terms). 'Unlawful activity' is potentially of wide application, and it is not 100% clear whether the 'investigation' has to be purely internal to fall within the exception.

59 Under the Australian NPPs, (above n 6) the relevant exception would be NPP 2.1(g) – the 'use or disclosure is required or authorised by or under law'.

60 *Totalise Plc v The Motley Fool Ltd, Interactive Investor Ltd* [2002] 1 WLR 1233; [2002] FSR 50, esp paras 26-28. The reasoning in the case, it should be noted, was based to a significant extent on the *Human Rights Act* 1998 (UK) and the *Data Protection Act* 1998 (UK). There is no guarantee that such an approach would be adopted in Australia. On the contrary, in the one NSW Supreme Court case that has mentioned the *Totalise* decision, the judge did not appear inclined to agree with its reasoning: *Airways Corporation of New Zealand v The Present Partners of Pricewaterhouse Coopers Legal* [2002] NSWSC 521

61 One of the reasons which Verizon has given in the proceedings in the United States is the fear of a flood of automated requests for information from copyright owners: see Verizon, *Opposition of Verizon Internet Services to Motion to Enforce Ex Parte Subpoena Issued July 24, 2002,* 30 August 2002, available at http://www.eff.org/Cases/RIAA_v_Verizon/20020903_verizon_opposition.pdf (last visited 28 October 2002). See also Yeng, above n 3.

62 The Electronic Frontiers Foundation (EFF) maintains a website with links to information on this case: http://www.eff.org/Cases/RIAA_v_Verizon/ (last visited 28 October 2002). The case has attracted media attention in the United States: see eg Krim, Jonathan, *A Story of Piracy and Privacy,* The Washington Post, 5 September 2002.

63 Specifically, 17 USC §512(h).

64 See generally Bygrave, Lee, 'The Technologisation of Copyright: Implications for Privacy and Related Interests' [2002] 2 *EIPR* 51; Cohen, Julie, 'The Exclusive Right to Read' (1996) 28 *Connecticut L Rev* 981

65 *NPP* (above n 6), NPP 1.1

66 *Directive 2001/29 of the European Parliament and of the Council of May 22, 2001 on the harmonisation of certain aspects of copyright and related rights in the information society* [2001] OJL167/10ff, esp Recital 57.

67 Samuelson, 'Intellectual Property and the Digital Economy: Why the Anti-Circumvention Regulations Need to be Revised' (1999) 14 *Berkeley Technology L Jo* 519, at 553ff

68 Copyright Law Review Committee, *Copyright and Contract* (2002), available at www.clrc.gov.au (last visited 28 October 2002).