

COMPREHENSIVE GUIDE TO
PRIVACY LAW
— PRIVATE SECTOR —

UPDATE SUMMARY

Update 6: 15 August 2005

Commissioner's report into review of Privacy Act released

The Attorney-General published the Federal Privacy Commissioner's 345 page report on her review of the operation of the private sector provisions of the *Privacy Act 1988* (Cth), entitled *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988*, in May 2005. Overall, the Commissioner found that the private sector provisions "work well" and that there is no need for fundamental change. Generally, business is satisfied with the provisions which have met some, but not all, of their objectives. In particular, the provisions do not appear to have met their objectives of establishing a national privacy scheme or of resolving international concerns regarding the level of privacy protection in Australia.

The report makes 85 recommendations as to how the Act can be improved. However, many of the recommendations are couched in the terms "The Government should consider" conducting a course of action and, as such, are more akin to outlining options rather than making recommendations. This could have a significant impact on the 'forcefulness' of the report and the extent to which the Government will make changes based on it.

Some of the major recommendations that would, if adopted by the Government, have a significant impact on business include merging the NPPs and IPPs, transferring Part 13 of the Telecommunications Act to the Privacy Act, excluding telecommunications businesses (including ISPs) from the small business exemption, including the National Health Privacy Code in the Privacy Act, requiring organisations to disclose from where they obtained a person's information, establishing a direct marketing do-not-contact register, simplifying the privacy code approval process, amending the definition of a small business to a business with 20 employees (as opposed to \$3m turnover) or less, requiring organisations to ensure information disclosed to contractors is protected and allowing disclosures during due diligence.

A detailed eight page summary of the Commissioner's report is included at [37-7920].

Senate report into review of Privacy Act

The Senate Legal and Constitutional References Committee completed and released its report into the *Privacy Act 1988* in June 2005. The 174 page report, entitled *The Real Big Brother: Inquiry into the Privacy Act 1988*, makes 19 recommendations regarding changes that should be made to the Act.

Overall, in contrast to the Privacy Commissioner's report, the Committee concluded that the Act is not providing effective or appropriate privacy protection due to a range of factors that undermine its operation, including a lack of consistency with other legislation, a lack of relevance to emerging technologies, the Act's numerous exemptions, a shortage of funding for the Privacy Commissioner and inadequate complaints handling and enforcement mechanisms. The Committee expressly stated that it disagreed with the Federal Privacy Commissioner's conclusion that the provisions are "working well". Whilst the Committee generally endorsed the Commissioner's recommendations, it stated that the Commissioner "could have gone further" in many cases. As such, many of the Committee's recommendations go beyond those of the Commissioner and, if adopted by the Government, will have a significant impact on the operation of the Privacy Act. These include recommendations regarding: changing the meaning of personal information to include information that enables an individual to be contacted (as opposed to only identified); removing the exemptions relating to small businesses, employee records and political acts and practices; penalising organisations that misrepresent the Privacy Act (eg. by falsely claiming information cannot be disclosed because of privacy laws); requiring direct marketing to be opt-in; and not making proposed changes to allow positive credit reporting.

A detailed summary of the report is included at [37-7930].

Workplace Surveillance Bill 2005 (NSW)

The *Workplace Surveillance Bill 2005* (NSW) was assented to on 23 June 2005. The commencement date is not yet known. In an Australian first, the Workplace Surveillance Act

effectively extends the regulatory scheme that was established under the *Workplace Video Surveillance Act 1998* (NSW), which it replaces, to also cover employee surveillance by means of computer surveillance and tracking surveillance. Generally, the Act:

- places a general prohibition on video, computer and tracking surveillance of employees unless employees have been notified or a covert surveillance authority has been obtained;
- prohibits surveillance of employees whilst they are not at work except in relation to computer surveillance of work equipment and resources (eg. laptops and internet accounts);
- prohibits employers from blocking delivery of an email or access to a website unless:
 - the employer has a policy on email and internet access and is acting in accordance with that policy (although, a policy cannot provide for blocking merely because the email or website relates to industrial matters); and
 - in the case of blocking an email - the employee is issued a “prevented delivery” notice except in relation to certain emails such as spam and offensive emails; and
- regulates how information and records obtained from surveillance may be handled.

Overall, the Act is not overly restrictive regarding overt surveillance practices as, provided notification requirements are met, the manner in which overt surveillance is conducted is left unregulated. As such, an employer is largely free to conduct overt surveillance in any manner that it chooses. Organisations that have already adopted best practice standards regarding overt workplace surveillance will only need to make minor adjustments to ensure compliance. Obligations are, however, more onerous in relation to the conduct of covert surveillance.

A detailed guide to the Act, along with commentary, compliance tips, sample policies and a comprehensive compliance checklist, is included at [208-1].

Commissioner pro-active against bundled consents

In the Privacy Commissioner’s report into her review of the private sector provisions of the Privacy Act (above), the Commissioner indicated that she will develop guidelines regarding the use of bundled consents in view of the desirability of lessening the incidence of their use (in relation to bundled consents generally, see [40-1660]). Similarly, in recently published speech notes (*Bundled Consent and the Review of the Private Sector Provisions*, Australian Credit Forum Privacy Seminar, 20 July 2005) the Commissioner indicated that, in her opinion, bundled consents may be contrary to the spirit of the Privacy Act. Further, in *OPC v Employment Services Company* [2005] PrivCmrA 13 (below), the Commissioner was pro-active in discouraging use of bundled consents by the respondent, despite the fact that they are permitted under the Act. These moves suggest that the Commissioner is seeking to limit the use of bundled consents by organisations. In view of this, organisations may choose to consider only using bundled consent forms where strictly necessary in the future and possibly reviewing existing forms to see if they can be “unbundled” in any way.

Federal Privacy Commissioner’s latest case notes

The Commissioner has released eight case notes relevant to the private sector:

- ***OPC v Employment Services Company*** [2005] PrivCmrA 13: The respondent, an employment services company, had been requiring applicants to provide a large amount of personal information (including tax file numbers (“TFNs”) and credit card details), was photocopying applicants’ passports and was requiring applicants to sign bundled consent forms regarding a wide range of uses and disclosures of their information. The Commissioner commenced an own motion investigation. *Outcome:*
 - Collecting TFNs from applicants before they were accepted for registration was not authorised by taxation, assistance agency and superannuation law and, as such, breached TFN Guideline 5.1 (see [22-610]). The respondent removed the requests on application forms for TFNs.
 - The photocopying of passports breached NPP 7.2 (“Identifiers”) as it constituted use of passport numbers (ie. Commonwealth identifiers) in circumstances not permitted under that principle (see [7-5250]). The respondent agreed to sight passports in future rather than copy them.
 - Requiring applicants to provide credit card details on application forms was an unnecessary collection of information and breached NPP 1.1 as an applicant had the

option of paying fees by means other than credit card. The respondent removed the requests on application forms for credit card details.

- The Commissioner “raised concerns” with the respondent that its collection statement required applicants to consent to a broad range of uses and disclosures of information which may not have been necessary. The Commissioner advised that such bundled consent forms diminish individuals' freedom of choice, coercing them to hand over their information. The respondent reviewed its consent form to remove references to unnecessary uses and disclosures and reviewed its application forms to enable applicants to opt-in to future uses and disclosures that were unrelated to their placement with employers.

Reported at [22-610], [7-166], [7-5253] & [40-1660].

- **K v Credit Provider** [2005] PrivCmrA 8: The complainant had the option of either purchasing a vehicle at the end of a lease arrangement by paying the residual amount or returning the vehicle to the credit provider. Following non-payment, the complainant was provided seven days to make payment or return the vehicle. A second deadline was later set but missed. The complainant advised that they would pay the full amount in four days, however, the credit provider demanded the return of the vehicle which the complainant refused to do. The credit provider visited the complainant's recorded place of residence, but was told he no longer lived there. The credit provider listed the amount owed on the complainant's consumer credit information file as a “clearout” (a “serious credit infringement”). Section 18E(8)(a) of the Act provides that information may be included on a credit information file if it is a record of a credit provider's opinion that the individual has committed a “serious credit infringement”. The complainant indicated the outstanding amount would be paid in four days but only paid the debt eight days later. The complainant disputed their address details had changed. The credit provider and complainant had been in phone contact leading up to the clearout listing. *Outcome:* The complainant's actions did not indicate to a reasonable person an intention to no longer comply with their obligations in relation to the debt owed and, as such, did not constitute a “serious credit infringement”. The credit provider's listing breached s.18E(8)(a). The credit provider agreed to remove the listing. See [19-1060].
- **L v Insurer** [2005] PrivCmrA 9: The complainant lodged a complaint about an insurance company that was a signatory to the *General Insurance Information Privacy Code* (“GIIP Code”). The GIIP Code provided that complaints may be made to Insurance Enquiries and Complaints Ltd (“IEC”). *Outcome:* The Commissioner was unable to investigate the complaint and referred it to the IEC as s.36(1A) of the Privacy Act generally prevents a person from lodging a complaint with the Commissioner about an organisation that is bound by an approved privacy code if the code contains a procedure for handling complaints (see [34-530]). In such a case, the complaint must be lodged in accordance with that procedure. See [34-530].
- **OPC v Banking Institution** [2005] PrivCmrA 11: The respondent, a banking institution, had an internal fax number for receiving customer information from staff. Staff occasionally mis-keyed the fax number causing the information to be sent to another organisation. The other organisation's business involved collecting and automatically forwarding information to its customers. On at least two occasions, the organisation received and automatically forwarded to its own customers the respondent's customer information. The Commissioner commenced an own motion investigation pursuant to s.40(2) on the grounds that the problem had happened before and may be systemic. *Outcome:* The respondent stopped using a facsimile-based service and introduced a secure on-line service and permanently decommissioned the fax number. The other organisation blocked all faxes other than those from designated numbers. Reported at [7-909] & [7-3141].
- **P v Telecommunications Service Provider** [2005] PrivCmrA 15: The complainant had a silent mobile number and subsequently acquired a secondary mobile number for use with the existing handset for the transmission of data associated with wireless access protocol capability. This data transmission number was listed as a mobile number in a public phone directory beside the complainant's previously undisclosed name and address which had been included in error. *Outcome:* The disclosure breached NPP 2 (“Use and disclosure”) as it was not permitted under any of the exemptions to that principle and, in particular, was not

permitted under NPP 2.1(a) as being a related secondary disclosure within reasonable expectations (see [7-910]). NPP 4 (“Data Security”) was also breached as there was a systemic flaw in the respondent’s software that led to the disclosure and reasonable steps had not been taken to protect the complainant’s information. The respondent paid an undisclosed amount of compensation, implemented new audit procedures in order to identify and minimise errors and ceased forwarding clients’ silent mobile details to the publisher of the telephone directory in order to reduce the risk of unauthorised publication. Reported at [7-937] & [7-3142].

- **Q v Credit Provider B** [2005] PrivCmrA 16: Credit provider “A” listed an overdue account on the complainant’s consumer credit information file. The listing was purged after five years in accordance with s.18F of the Privacy Act (see [19-1260]), despite it remaining unpaid. The debt was sold to credit provider “B” who, three months later, listed the debt on the complainant’s credit information file. The applicable statutory limitation period to commence legal proceedings to recover the debt was six years, however, more than six years had passed since the cause of action arose. Paragraph 2.8 of the *Credit Reporting Code of Conduct* prohibits a credit provider listing a statute-barred debt (see [19-5140]). Further, paragraph 55A of the Explanatory Notes to the Code provides that this prohibition includes the re-listing of information after the maximum period permitted for the retention of such information on a credit information file has expired (under s.18F). *Outcome*: Credit provider B breached the Code as the information had been re-listed after the expiry of the maximum period permitted for its retention (under s.18F) and after the statutory limitation period had expired. Credit provider B acknowledged its error, removed the listing and apologised to the complainant. Reported at [19-5140].
- **R v Internet Service Provider** [2005] PrivCmrA 17: The complainant held an account with the respondent, an internet service provider. The respondent reset the password for the account at the request of a third party purporting to be the complainant and without following, in full, its standard procedures which involved asking a series of security questions. The third party accessed the account causing the complainant significant personal difficulties. *Outcome*: Whilst the respondent had security procedures in place, the procedures were not correctly or consistently followed. The respondent breached NPP 4.1 (“Data Security”) by failing to follow its procedures correctly or consistently as this constituted a failure to take reasonable steps to protect the information from misuse and loss and from unauthorised access, modification and disclosure.
The Commissioner also found that, in resetting the password in the absence of the complainant’s consent, the respondent had improperly “disclosed” the complainant’s information to the third party in breach of NPP 2 (“Use & Disclosure”). This is significant as, whilst not all of the facts of the case are clear from the Commissioner’s case-notes, it appears that, as the respondent does not appear to have provided the third party with information (but, rather, confirmed the correctness of information provided by the third party and confirmed that the new password assumedly nominated by the third party had been activated), a “disclosure” under NPP 2 covers these types of circumstances. The Commissioner conciliated the matter, which concluded with a confidential settlement between the parties. Reported at [7-909:1A] & [7-3143].
- **S v Credit Provider** [2005] PrivCmrA 18: The complainant obtained a business loan from a credit provider which it did not fully repay. The credit provider listed a payment default on the complainant’s consumer credit information file. The complainant paid the outstanding amount and requested the credit provider to amend the credit file. The credit provider refused, claiming other fees were still outstanding. The complainant provided proof of payment to the credit reporting agency which updated the credit file. *Outcome*: The credit provider breached s.18E(8)(a) of the Privacy Act by listing the payment default on the complainant’s consumer credit information file as the loan was for commercial purposes whereas only consumer credit information is permitted to be listed on such a file (see [19-660] & [19-980]). The listing was removed from the complainant’s file. The Commissioner sought from the credit provider written evidence that its staff were provided with training on the operational guidelines of the credit reporting agency as well as training in the operation of the credit reporting provisions of the Privacy Act. The credit provider also provided a written apology. The complainant sought compensation, however, the Commissioner asked the complainant to substantiate such a

claim. The complainant failed to reply to the request. The Commissioner closed the investigation on the basis that it had been adequately dealt with by the credit provider. Case reported at [19-660].

No breach by doctors disclosing de-identified info:

The Privacy Commissioner conducted an investigation into the disclosure of patient information by doctors to CAMM Pacific (“CAMM”) via Health Communications Network Ltd’s (“HCN”) “Medical Director” software. CAMM was conducting a study aimed at collecting data about promotional activities sponsored by pharmaceutical companies. CAMM received information from HCN which had itself received the information from doctors via the Medical Director software. It had been alleged to the Commissioner that an extraction tool that removed information from the Medical Director software was faulty because it extracted the patient information of all doctors working in group practices, even those who had not elected to participate in the extraction exercise. *Outcome:* The Commissioner found that there had been no breach of the Act as patient information transferred from the doctors to CAMM via the software was de-identified and, as such, did not fall within the meaning of personal information under the Act. If a medical practice accidentally transferred de-identified patient records of a non-consenting doctor, HCN could not identify that doctor and did not use the de-identified patient information. Reported at [7-909:1B].

Privacy Act does not prevent discovery of third party documents

In *Tan v St George Bank* [2005] WASC 143, the Supreme Court of W.A. considered whether discovery should be ordered where documents contained confidential information about third parties and whether this would be permitted under the *Privacy Act 1988* (Cth). The Court noted that the right of privacy conferred by the Act is not inviolable, as is recognised by NPP 2.1(g) which permits disclosure of information if required or authorised by law. It is also the case that, if discovery was ordered, measures could be taken to cover over the names of the third parties and other details that might identify them. See [40-6742].

ABC unable to rely on Privacy Act’s journalism exemption

In *Rivera v Australian Broadcasting Corporation* [2005] FCA 661, the ABC sought to rely on the journalism exemption under s.7B(4) of the Privacy Act in defence to proceedings that had been brought against it regarding an alleged privacy breach resulting from a show it had broadcast. The ABC claimed that, as required under the exemption, it was publicly committed to observe privacy standards that have been published in writing by virtue of its “ABC Editorial Policy”. However, the ABC failed to tender those standards in evidence. The ABC merely provided a copy of its Online Privacy Policy as evidence. Despite the fact that the ABC fell within the meaning of a “media organisation” under the Act, Hill J held that the ABC had not adduced sufficient evidence to exclude any of its acts under the journalism exemption. The ABC appears to have committed a similar error to that which occurred in *Kadian v Richards* [2004] NSWSC 382 (see 34-63) in which the plaintiffs failed to establish that two doctors were bound by the NPPs as they did not first establish that the doctors were not bound by an approved privacy code, as required under s.16A of the Act. These cases highlight that organisations must ensure that evidential burdens regarding the Act’s coverage are met before seeking to rely on its provisions. Commentary on *Rivera* is included at [3-1012].

Privacy breaches of Commercial TV Industry Codes

- The ABA found that *Network Ten Brisbane* (TVQ Brisbane) breached cl. 4.3.5 of the *Commercial Television Code of Practice 2004* by revealing the names of a child and parent in a news item on bullying in schools and cl. 4.3.5.1 by failing to exercise special care before using material relating to a child’s personal or private affairs. Network Ten conducted code training with the relevant newsroom and undertook to bring the finding to the attention of all news staff. Reported at [98-2227].
- The ABA found that a 60 Minutes segment breached a complainant’s privacy, under cl. 4.3.5 of the *Commercial Television Industry Code of Practice 1999*, by showing footage of the complainant partaking in an exorcism without her knowledge or consent. Nine Network undertook to circulate and discuss the ABA’s finding with 60 Minutes producers and reporters and to use the finding as an example in ongoing training regarding application of the Code. Reported at [98-2227].

In view of the large number of media privacy complaints, summaries of all investigations by the ABA (now the ACMA) into alleged privacy breaches by commercial TV stations (dating back to November 1998) have been included at [98-2227].

SCNSW limits media intrusions to protect privacy

In *John Fairfax Publications v Ryde Local Court* [2005] NSWCA 101, a media organisation sought access to court records relating to apprehended domestic violence order proceedings. The Supreme Court of NSW analysed in detail the need for laws to protect individuals' privacy against intrusions from powerful private sector organisations and, in particular, media organisations. In a key passage, Spigelman CJ stated (at [77]):

The common law has a long tradition of protecting persons' right to privacy. I reiterate the observations I made in TCN Channel Nine Pty Ltd v Anning (2002) 54 NSWLR 333 at [59]-[61]:

"Although the law has been particularly protective of persons from intrusion on the part of the organs of government, it should be no less protective in the case of other powerful sections of society of which, in contemporary conditions, the mass media is one....."

In refusing access, Spigelman CJ, with whom the other judges concurred, cited various other authorities supporting this point. See [98-2239].

Privacy breach to obtain address does not invalidate notice

In *Matheson v Scottish Pacific Business Finance Pty Ltd* [2005] FCA 670, the Respondent obtained a judgment against the applicant who was one of its debtors. A bankruptcy notice was issued when the judgment debt was not paid. The applicant appealed the making of a subsequent sequestration order on the grounds that the original creditor (who later factored the debt to the Respondent) acted in contravention of the *Privacy Act 1988* regarding the manner in which it obtained his residential address in order to serve him with the originating proceedings. The applicant claimed that such unlawful conduct "tainted" the claim for the debt with illegality. The Court held that, even if there had been a breach of the Act, it did not affect the validity of the debt. Reported at [7-82].

ACA registers E-marketing Code of Practice

On 16 March 2005, the Australian Communications Authority ("ACA") (now the ACMA) registered the *Australian eMarketing Code of Practice* under s.117 of the *Telecommunications Act 1997* (Cth). The Code sets industry-wide rules and guidelines for the sending of commercial electronic messages in accordance with the *Spam Act 2003* and aims to set higher standards of practice than those required under the Act. An e-marketer does not have to be a signatory to be bound by the Code. Commentary regarding coverage, enforcement and complaint handling included at [98-45].

English courts uphold right to privacy against media

In *Douglas v Hello!* [2005] EWCA Civ 595 (relating to the unauthorised publication of wedding photos - for facts of the case, see [490-1700]), the English Court of Appeal ("ECA") reconfirmed that privacy interests in England will be protected under laws of confidence. However, the decision was based on the application of European Community law and U.K legislation that does not have any equivalent in Australia.

In reviewing the question of privacy, the Court followed the landmark decision of the European Court of Human Rights ("ECHR") in *von Hannover v Germany* (24 June 2004) in which the ECHR considered whether photos of Princess Caroline of Monaco in public places infringed her privacy. The ECHR held that national courts of States bound by the *European Convention for the Protection of Human Rights and Fundamental Freedoms* have a duty to protect privacy of individuals under Article 8 of the Convention. In applying that decision, the ECA found that it was under an obligation to interpret the *Human Rights Act 1998* (U.K.) in a way that would protect the privacy of individuals and the cause of action under which to do this was breach of confidence. In view of this, it is likely that English Courts will increase the level of protection afforded to privacy interests by continuing to develop the laws of confidence in this manner (for commentary on how the laws of confidence have already been adapted to protect privacy interests, see [490-1690]). The Court also indicated that the original interlocutory injunction preventing *Hello!* from publishing the unauthorised photos should have been upheld as damages for mental distress resulting from

the invasion of privacy was an inadequate remedy. As such, it is likely that injunctions will be awarded more readily by English Courts in privacy cases, having significant implications for media organisations. Case reported at [490-1700].

Other developments

- **“Held” does not include “held” in mind of employee:** In *Vice-Chancellor Macquarie University v FM* [2005] NSWCA 192, it was found that “held” under the *Privacy and Personal Information Protection Act 1998* (NSW) does not include information “held” in the mind of an employee. However, unlike the *Privacy Act 1988* (Cth), the NSW Act does not expressly require information to be held in a material form. See [3-1810].
- **Victoria considers Bill of Rights to protect privacy:** Victoria is considering implementing a Bill of Rights to establish, amongst other things, a statutory right to privacy. Victorian Attorney-General, Rob Hulls, released a discussion paper, entitled *Have your say about human rights in Victoria*, in June 2005. A Human Rights Consultation Committee has been formed to conduct the review. The Committee will report to the Government by 30 November 2005. The discussion paper is available www.justice.vic.gov.au/humanrights.
- **SCV orders disclosure of abortion records:** In *Royal Women's Hospital v Medical Practitioners Board* [2005] VSC 225, the Supreme Court of Victoria held that the Medical Practitioners Board of Victoria (“Board”) should have access to a woman’s abortion records. On 8 October 2004, the Melbourne Magistrates Court dismissed an application by the Royal Women’s Hospital (“RWH”) to prevent the disclosure of the records to the Board, finding that the medical records of a public hospital are not immune from production. The Board was investigating the conduct of doctors at the RWH who performed the abortion while the woman was 32 weeks into her pregnancy. Amongst other things, the Court held (reported at [79-860]):
 - the doctor-patient confidential relationship will not withstand the law compelling disclosure to give evidence or to provide documents;
 - s.28(2) of the *Evidence Act 1958* (NSW), which restricts a medical practitioner from divulging information obtained for the purposes of treatment in a “civil suit action or proceeding”, generally only applies to court proceedings and does not apply to an investigation under the *Medical Practice Act 1994* or a hearing conducted by the Board;
 - s.141(2) of the *Health Services Act 1988* (NSW), which makes it a criminal offence to give information to another person in certain circumstances, does not prevent disclosures required by law, such as pursuant to a warrant or court order;
 - the public interest in the proper investigation of the matter outweighed the public interest in the RWH maintaining the confidentiality of the information.
- **Narrow interpretation of interceptions legislation:** In *NSW Crime Commission v Vuletic* [2005] NSWSC 614, the Supreme Court of N.S.W. adopted a narrow interpretation of s.47 of the *Telecommunications (Interception) Act 1979* (Cth) which generally requires interceptions by law enforcement agencies pursuant to certain warrants to take place as a result of an “employee” of the carrier involved. The case is significant as it follows the significant body of case law which indicates that, in view of the privacy considerations with which the Act is concerned, exemptions under the Act are to be interpreted narrowly. See [127-2710].
- **Software error causes privacy breach by law firm:** High profile law firm, Slater & Gordon, was reported in the media to have admitted that a software error caused a privacy breach on its website causing the personal details of online job applicants to be revealed. It was reported that the firm took immediate corrective action and apologised to the persons affected and that the Privacy Commissioner had been in contact with the firm regarding the incident.
- **Liberal party telemarketing activities exempt under Privacy Act:** The ACA concluded in late March 2005 an investigation into telemarketing activities by the Liberal Party of Australia during the 2004 federal election campaign. The ACA found no evidence of misuse of data from the Integrated Public Number Database (IPND) and that phone numbers had been obtained from publicly available databases. The Privacy Commissioner declined to investigate the complaint on the basis that the Liberal Party’s activities were exempt under the political acts and practices exemption under s.7C of the *Privacy Act 1988*. Reported at [3-1060].

- **Car business fined under Spam Act:** The operator of www.carsales.com.au was fined over \$6,500 by the Australian Communications Authority (“ACA”) in April 2005 for sending text-messages promoting its website to people who had advertised their vehicles (along with their mobile phone numbers) in newspaper classifieds. The ACA believed that the mobile numbers were published by vendors only so potential buyers could contact them and that they did not consent to receiving text messages from a car sales website with which they had no prior business relationship. As at 5 April 2005, the ACA indicated that it had required 200 businesses to amend their practices to comply with the Spam Act. Of those required to change their practices, three have been fined for more substantial breaches, three have been issued with formal warnings and one has given an enforceable undertaking. Reported at [98-40].
- **Fed Ct issues interim injunctions under Spam Act:** In *Australian Communications and Media Authority v. Clarity1 Pty Ltd and Wayne Robert Mansfield* (No. WAD 155 of 2005), the Federal Court issued interim injunctions (until a further hearing in August 2005) under the *Spam Act 2003* against Clarity1 Pty Ltd of Perth and its managing director, preventing them from sending commercial electronic messages otherwise than in accordance with the Spam Act. When requesting the injunction, the AMCA alleged that Clarity 1 sent over 50 million spam emails in the 12 month period following the commencement of the Act. In early May 2005, the ACA had executed a search warrant on the premises of an unnamed Perth company as part of an investigation under the Spam Act. It is likely that the unnamed company was Clarity1.
- **UN working group releases report on internet governance:** On 14 July 2005, an independent working group established by the UN released a report on the governance of the internet, the conclusions of which will be considered during the second phase of the World Summit on the Information Society (WSIS), to be held in November 2005 in Tunis. The report makes recommendations in a number of policy areas, including data protection and privacy rights regarding which it recommended: (a) encouraging countries that lack privacy and personal data protection legislation to develop clear rules and legal frameworks to protect citizens against the misuse of personal data; (b) revising the policies governing the WHOIS databases to take into account the existence of applicable privacy legislation in the countries of the registrar and of the registrant; (c) defining policy and privacy requirements for global electronic authentication systems and developing open technical proposals for electronic authentication that meet such requirements; and (d) discussing a broad set of privacy-related issues described in the Background Report so as to define practices to address them. The report also contained recommendations regarding security, cybercrime and spam. The report is available at www.itu.int/wsis/wgig/index.html.
- **RACGP releases Standards for General Practices (3rd ed):** The Royal Australian College of General Practitioners (RACGP) released a third edition of its non-binding *Standards for General Practices* in late June 2005. The standards address a range of patient privacy issues, including: patient health records (1.7.1); presence of third parties (2.1.3); confidentiality and privacy of health information (4.2.1); information security (4.2.2); transfer of patient health information (4.2.3); and retention and destruction of patient health information (4.2.4). The Standards are available at www.racgp.org.au. Reported at [70-617].
- **A.C.T. Human Rights Commission:** The *Human Rights Commission Bill 2005* (A.C.T.) has been introduced into the A.C.T. Legislative Assembly to establish a new A.C.T. Human Rights Commission (“HRC”). The Commission will bring together the Human Rights Office and the Community and Health Services Complaint Commission. Currently, under the *Health Records (Privacy and Access) Act 1997* (“HRPAA Act”), complaints are lodged with the Community and Health Services Complaint Commission. Amongst other things, the *Human Rights Commission Legislation Amendment Bill 2005* (A.C.T.) makes the necessary consequential amendments to the HRPAA Act to allow the HRC to undertake those tasks in the future.
- **EU papers on privacy, RFID & intellectual property:** The European Union Article 29 Data Protection Working Party released two working papers earlier this year regarding data protection issues related to:
 - (a) *RFID technology:* The paper provides guidance to manufacturers of the technology (RFID tags, readers and applications) as well as RFID standardisation bodies on their responsibility

towards designing privacy compliant technology in order to enable deployers to carry out their obligations under the data protection Directive (reported at [297-560]).

(b) *Intellectual property rights*: The paper analyses privacy issues in the context of the deployment of on-line services using digital rights management systems (“DRMSs”) and the processing of data to conduct investigations into suspected copyright infringements.

The papers provide useful resources for Australian organisations dealing with RFID technologies and DRMSs. The papers are currently available at:

www.europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/consultations/index_en.htm

UPCOMING DEVELOPMENTS

A-Gs release discussion paper on unauthorised internet photos

The Standing Committee of Attorneys-General released a discussion paper, entitled *Unauthorised Photographs on the Internet and Ancillary Privacy Issues*, on 9 August 2005 in response to concerns regarding the way unauthorised photographs are being used on the internet. The Discussion Paper seeks to identify the issues associated with such publications, discuss the adequacy of existing laws and identify options to address these issues. The Paper is available at www.ag.gov.au. Submissions close on 14 October 2005.

Draft IPND standard

The ACA released a draft *Telecommunications (Use of Integrated Public Number Database) Industry Standard 2005* on 25 May 2005 following concerns that customer information was being used for purposes beyond those permitted under Part 13 of the *Telecommunications Act 1997*. The standard will be mandatory and will protect the contact information (name, address and telephone number) of telecommunications customers held in the Integrated Public Number Database (IPND) from inappropriate use, disclosure and access. The draft standard is available at www.acma.gov.au.

Democrats’ Spyware Bill

The Australian Democrats introduced a *Spyware Bill 2005* on 12 May 2005. Spyware is software that installs itself on computers without the knowledge of the user and reports to the sender about the user’s online behaviour. It is uncertain whether the Bill will be passed, particularly in view of the legislative review by the DCITA and the A-G’s Department earlier this year which concluded in March that statutory changes were not required to address spyware issues. The Bill requires senders of spyware to seek consent to install and use it and to explain what and how information will be used. Once installed, the spyware must make it easy for the user to remove or uninstall it or to turn it off. The Bill contains exemptions relating to network security and software that is contained on computers at the time of retail sale.

DISCLAIMER:

Presidian Legal Publications takes the greatest precautions to ensure that its publications are correct, accurate and up to date. However, it is a condition of purchasing, accepting or using this publication that: (a) the publication is not intended to be, nor constitutes, legal or other professional advice and is merely a research guide to the area of law to which it relates; (b) where a purchaser, reader or other person (“User”) uses the publication for any purpose, including a purpose in relation to the provision of legal or other professional advice, the User must first verify the accuracy and currency of information in, and any other materials obtained from, the publication (eg. with primary legislative sources); and (c) the authors, editors, consultants, researchers, endorsers, contractors and every other person involved with the compilation, writing or supply of this publication, are excluded from all liability for any form of loss or damage (“Loss or Damage”) suffered by any person, group, association, body corporate or User as a result of any error or omission within, or use of or reliance on, this publication, and, as such, and without limiting the generality of the preceding clauses, are not liable for any direct, indirect, consequential or special damages or damages for lost profits in relation to any such Loss or Damage.