The Inside Word

ESSENTIAL NEWS ON PRIVACY ISSUES

SPECIAL BRIEFING : Data security in practice

➢ A review of NSW cases on the Security principle

NSW privacy law has two Security principles:

- IPP 5 (s. 12) in the *Privacy and Personal Information Protection Act 1998* – covering non-health personal information in the public sector, and
- HPP 5 (Schedule 1) in the *Health Records and Information Privacy Act 2002* – covering health information in the public and private sectors.

All cases mentioned in this briefing relate to IPP 5. However the conclusions drawn apply equally to HPP 5, as the two principles are virtually identical in their wording. (The only differences are to accommodate "personal information" versus "health information", and "agencies" versus "organisations".)

IPP 5 and HPP 5 each incorporate retention and disposal requirements in paras (a) and (b), plus a requirement relating to contracted services in para (d). However the focus of this briefing is para (c), which states that an agency (or organisation) must ensure that the personal information (or health information) it holds:

is protected, by taking such security safeguards as are reasonable in the circumstances, against loss, unauthorised access, use, modification or disclosure, and against all other misuse.

A number of NSW cases have examined this requirement to take "such security safeguards as are reasonable in the circumstances".

What we can draw from the NSW case law is, not surprisingly, that the appropriate security safeguards will depend on the circumstances of the case. This may include the sensitivity of the information being held, with specific reference to the presence of medical records, for example, signalling "the need for greater confidentiality" (*MT v Director General NSW Department of Education & Training* [2004] NSWADT 194 at [178]).

Physical and administrative safeguards

Storing paper student files in a space accessible to all teachers and administrative staff has been found to indicate a security failure, as was the failure to have a policy about restricting access to paper files, and the absence of any system of staff training about privacy (*MT*, as above).

Other cases have featured orders for an agency to revise its privacy policies and procedures, and implement staff training – even if the Security principle was not found to have been breached in that instance (*SW v Forests NSW* [2006] NSWADT 74).

In *RD v Department of Education & Training* [2005] NSWADT 195, sensitive medical information about an employee had been mailed to the wrong address – twice – because of a failure to check the employee's address. Although this case turned on the Accuracy principle rather than the Security principle, the Tribunal nonetheless ordered a change of security practices, ordering that all future mailings regarding medical assessments of employees be sent by registered mail.

Another case concerned itself with the transfer of information in the courtroom, between a prosecution team and a defence team. Although the Tribunal warned that care should be taken in the handing over of sensitive information in public settings such as the body of a court room at hearing, the Tribunal found no breach of IPP 5 in a systemic sense, because hand-to-hand transfers between lawyers bound by ethical requirements of confidentiality would ordinarily furnish an adequate level of security (*HW v Police* [2003] NSWADT 214 at [58]).

Technical safeguards

The Tribunal has said that, as a general rule, ex-inmate information should be held in a less active environment than current inmate records, and it should only be accessible to certain authorised officers (*FH v Corrective Services* [2003] NSWADT 72 at [26]-[28], [37]). This was not the practice in the NSW Department of Corrective Services when the Tribunal examined a privacy complaint in 2003.

However the Tribunal then took into account of "the evolutionary character of security practices, especially in a major operational environment". The Department escaped a finding of a breach of IPP 5 on the basis that while the security safeguards of their existing database may have been insufficient, the Department was apparently in an advanced stage of designing a new system, which would address this particular deficiency. The Tribunal did however note that if the new system was not implemented within the promised 12 months time frame, the Tribunal might in a future action form a different view (*FH*, as above, at [29], [30]).

In the same case but in relation to a slightly different data security issue, the absence of a 'log' to establish who had accessed files in a database was seen by the Tribunal as "less than adequate" and a "shortcoming". Nonetheless the respondent's assertion as to the multi-million-dollar cost of remedying this particular problem appeared to sway the Tribunal away from making a finding that the system breached IPP 5 (*FH*, as above, at [37], [41]).

Instead the Tribunal found that while there were "shortcomings", the system on the whole possessed adequate security, and stated:

"It is not … necessary to show that the security policies and practices are perfect or ideal in every respect. Where there are shortcomings, they have to be weighed in the balance alongside those aspects that are satisfactory. … The significance of the shortcomings need to be assessed by reference to the degree of risk that they carry for intrusion into the privacy of the persons whose data is secured, and the potential gravity of the consequences of any intrusion if it were to occur" (*FH*, as above, at [41]).

In another case involving the Department of Corrective Services, an issue arose as to what security safeguards are needed to prevent misuse by a 'rogue' employee – in this case, an employee who used her access to criminal record data to blackmail a convicted paedophile who was out on parole. The database she accessed included a user warning message stating:

"The information from the system now available to you is confidential and must NOT be disclosed to unauthorized persons under any circumstances, nor are you authorised to access such information for personal reasons".

The Tribunal found that this warning system constituted reasonable steps to prevent unauthorised access or misuse (*NS v Commissioner, Department of Corrective Services* [2004] NSWADT 263 at [21], [53]).

Another case involving data security related to personal information that had been unlawfully collected in the first place – digital photographs taken, apparently covertly, of a colleague in her pyjamas while away at a conference, then distributed on CD to various other parties. Here the agency had already moved to recover and destroy all the CDs, and undertook to conduct a further search of hard-drives and their network to find and destroy any remaining copies of the photographs. The Tribunal found that these actions constituted "reasonable security safeguards" to protect the information from any further misuse or disclosure, and so found no breach of IPP 5 (*SW v Forests NSW* [2006] NSWADT 74 at [42]).

Commentary

As the Security principle is aimed at preventing loss, misuse or unauthorised disclosure of personal or health information by addressing systemic points of weakness, an actual example of loss, misuse or unauthorised disclosure is not, in theory, required to prove a breach of IPP 5 or HPP 5. Nor will an example of actual loss, misuse or unauthorised disclosure necessarily mean there has been a systemic failing.

The Tribunal appears quite willing to chastise organisations over security failings that could have been prevented through commonsense and/or relatively inexpensive physical or administrative measures, and is certainly prepared to make a link between appropriate staff training and privacy policies, and compliance with data security requirements.

However the Tribunal appears equally mindful of the potential costs involved in technical fixes, in determining whether or not a database or network possesses 'reasonable' security. Nonetheless organisations should remain mindful of the opportunity presented by any major IT reviews, to upgrade privacy and security features in a timely and integrated fashion.

Briefing publication date: May 2006

For more information on the topics covered here, call Anna Johnston, Director of Privacy & Information Management Consulting, on (02) 9432 0320.