Symposium

Interpreting Privacy Principles: Chaos or Consistency?

17 May 2006

Sydney

Interpreting the Security Principle

Nigel Waters, Principal Researcher, interpreting Privacy Principles Project, Cyberspace Law and Policy Centre, University of New South Wales, nigelwaters@iprimus.com.au

This paper is a revised and updated version of an article entitled *IPPs examined: The Security Principle,* by Nigel Waters and Graham Greenleaf, published in Privacy Law & Policy Reporter Volume 11 No 3 in September 2004

Contents

Introduction

All privacy laws contain a security principle. There is clearly no point in having detailed rules about how personal information can be used and disclosed unless there is also an obligation to prevent unauthorised access. Such access can be either directly by unauthorised third parties (e.g. by hacking or phishing) or indirectly by unauthorised disclosure by someone with legitimate access. But the security obligation in privacy laws is also designed to protect against three other categories of risk: unauthorised use by authorised personnel, loss or corruption of data and other 'misuse'. See Figure 1.

Figure 1

For most individuals, damage or inconvenience from loss or corruption of data is probably more likely than from unauthorised access or use. However, individuals can suffer as much if not more damage due to information they need no longer being available when it should be as they can through misuse or unauthorised release. A good example is provided by a NZ case in which a hospital erased a video tape which was the subject of a disputed access request then under investigation by the Privacy Commissioner – the Commissioner negotiated a $5000 payment in compensation.[1]

[1] [1995] PrivCmrNZ Case Note 3984

Legislation

The security principles in most Australasian privacy laws are all very similar in effect though there are superficial differences. The first – IPP 4 in the federal *Privacy Act 1988* – has been the model for many of the others. It reads:

> "A record-keeper …. shall ensure that the record is protected, by such security safeguards as it is reasonable in the circumstances to take, against loss, against unauthorised access, use, modification or disclosure, and against other misuse .." (AusPA[2] s.14).

The NSW and NZ laws contain an almost identical principle (NSW PPIPA[3] s.12(c) – IPP5; NZPA[4] s.6 - IPP 5(a)).

The principle is simplified in the private sector NPPs, introduced into the federal Privacy Act in 2000:

> "An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure." (AusPA – NPP 4.1)

This formulation is also used in the Victorian *Information Privacy Act 2000* (Vic IPA[5] IPP 4.1), and in the Northern Territory *Information Act* (NT IA[6] IPP 4.1).

These security principles do not explicitly include as security breaches actions which are authorised by the record controller but still improper (for example, alteration of a person's record to frustrate an investigation). They only explicitly provide protection against 'access, use, modification or disclosure,' where it is unauthorised. However, both formulations include protection against 'misuse' or 'other misuse' *without* an express qualification that this can only occur through unauthorised acts.

It can be argued that these words encompass authorised but improper access, use, modification or disclosure, because it is otherwise difficult to give them any effect. The principles do not say that security breaches must be 'by someone else'. The alternative view, that the security principle only covers breaches 'by someone else' would provide a neater demarcation between the security principle and other IPPs. However, it is difficult to sustain this view because the references to 'loss' include destruction of personal

---

[2] *Privacy Act 1988 (Cth)* – abbreviated as 'AusPA' in this paper, to distinguish it clearly for international and lay readers from the Canadian and New Zealand Privacy Acts - CanPA and NZPA respectively

[3] *Privacy and Personal Information Protection Act 1998 (NSW)* – PPIPA herein

[4] *Privacy Act 1993 (NZ)* - NZPA in this paper

[5] *Information Privacy Act 2000 (Vic)* – Vic IPA herein

[6] *Information Act (NT)* – NT IA herein

information by the record-keeper or organisation itself. Privacy Commissioners have also taken the view that security must protect against those who have authorised access[7].

Special protection for sensitive information

Some privacy laws contain specific sensitive data principles which require additional measures to be taken in relation to certain types of information – typically health, criminal records, political views etc[8]. These principles generally deal with additional notification and consent requirements and are silent on security. But it remains implicit[9] in all the security principles that the sensitivity of the information is a factor to be taken into account in deciding on appropriate security.

The specific health privacy laws[10] which have been passed in some jurisdictions do not generally add any particular security obligations – the security principles in them simply restate the 'reasonable steps' requirement, leaving the standards to the judgement of the organisations holding health information. There do not appear to have been any cases involving these jurisdictions to date that add to our knowledge of the specific security measures that might be considered necessary when handling health information

One particular type of sensitive information is 'silent' or unlisted telephone numbers, which are often obtained because of a particular risk to the subscriber concerned. Two NZ cases have reinforced the need for particular care in securing unlisted numbers against unauthorised disclosure.[11] Canadian cases have highlighted the need for special protection for the Social Insurance Number (SIN)[12] and similar cases can be expected in those Australia jurisdictions that require special protection for government identifiers[13].

Most people would regard financial information as deserving of special attention, although it does not typically feature in the definitions of sensitive information in privacy laws. Reference has already been made above to recommendations for encryption of financial data, and the remedies awarded in some of the complaint cases probably reflect an appreciation by regulators of the importance most individuals attach to it, and also increasingly of the potential for fraudulent use of financial details. In a recent Canadian case, the Commissioner criticised the practice of sending unsolicited personalised

---

[7] For example see *E v Financial Institution* [2003] PrivComrA 3 (logging required).

[8] See *Privacy Act 1988 (Cth)* NPP 10; *Information Privacy Act (Vic)* IPP 10; *Privacy & Personal Information Protection Act 1998 (NSW)* s.19(1).

[9] Explicit in the Hong Kong Ordinance – DPP 4(a).

[10] *Health Records and Information Privacy Act 2002 (NSW)*; *Health Records Act 2001 (Vic)*; *Health Records (Privacy & Access) Act 1997 (ACT)*; *Health Information Privacy Code 1994 (NZ)*

[11] See [1997] PrivCmrNZ 12 (Cn10668) and [1994] PrivCmrNZ Case Note 0189

12 [2002] PrivCmrCan PIPEDA 69; [2003] PrivCmrCan PIPEDA 146.

[13] AusPA NPP7, and IPA IPP7

'convenience cheques' out with account statements.[14] While the case was settled on other grounds, it illustrates the potential for privacy laws to challenge widespread commercial practices on the grounds that they create an unacceptable risk of an interference with privacy, and other consequences.

'Reasonable steps' – sources of interpretation

A common feature of all the security principles in privacy laws is the qualification that the obligation is only to take 'reasonable' or 'reasonably practicable' steps – either expressly or implicitly related to the particular circumstances.

The guidance material issued by regulators offers advice on how to assess the 'reasonable' or 'practicable' level of security. The Federal and Victorian Privacy Commissioners' Guidelines[15] emphasise the need for a risk assessment. So too do the NSW government security guidelines which also suggest a 'baseline' level of precautions, with extra measures to deal with particular risks[16]. The federal Privacy Commissioner suggests that relevant factors in assessing risk include:

- The sensitivity of personal information
- The likely harm that could result from a breach
- The medium of storage; and
- The size of the organisation (larger organisations tending to need greater security)

Hong Kong is the only jurisdiction to include some of these factors in the text of the security principle in its law[17].

Organisations are understandably uneasy about such apparently subjective obligations and general advice. They will look ultimately to decisions of tribunals and courts for the standards required in different circumstances.

There are now a handful of decisions available which throw some light on what security measures might be held to be necessary. Examples of specific compliance measures considered by the regulators to be appropriate can also be found in the reports of conciliated cases published by some Privacy Commissioners, and in the reports of special

---

[14] See [2005] PrivCmrCan PIPEDA 299

[15] Office of the Federal Privacy Commissioner, *Guidelines to the National Privacy Principles*, September 2001, pp 44-46; Office of the Victorian Privacy Commissioner, *Guidelines to the Information Privacy Principles* Vol 2, pp 9-10.

[16] See http://www.oict.nsw.gov.au/content/2.3.16-Security-Pt1.asp

[17] *Hong Kong Personal Data (Privacy) Ordinance 1995.*

investigations and audits conducted by those Commissioners who have those functions[18]. These are considered in the rest of this paper.

Security is multi-faceted

The Australian Federal Privacy Commissioner makes a useful distinction between four different areas of security[19]: physical security; computer and network security; communications security; and personnel security. Organisations need to pay attention to all four of these areas to meet their obligations under security privacy principles. It is self evident that any security system is only as effective as its weakest component.

Another dimension to be considered is the storage medium – similar personal information is often stored within an organisation on paper, in central computer databases and on individual employees' workstations (including in Email) – all of these need to secured to an appropriate standard that avoids any 'weak links'. Computerisation is now so pervasive that it is all too easy to slip into assuming that the security discussion is about security solely of electronic data.

A particular dimension that now often needs to be considered is the internet environment, in which personal information that may have been been publicly available (whether mistakenly or not) is often replicated in mirror sites and web archives. A complaint about inappropriate disclosure conciliated by the Victorian Privacy Commissioner in 2003 involved the respondent contacting the operators of 'Google' to have personal information removed and links disabled, and required follow up action after several months to ensure that the action had taken effect[20]. This raises important issues of historical records/archives, which will be canvassed further in subsequent analysis of the retention and correction principles.

Security obligations are not absolute

No precautions can ever guarantee 100% security. There will always be clever individuals who can circumvent even the most elaborate security measures – whether in the physical or computer environments.

Nonetheless, organisations subject to privacy principles will be expected to have taken reasonable steps to secure personal information against ingenious unauthorised entry – whether to premises (breaking and entering) or to computer systems (hacking) – unless it

---

[18] The Federal Privacy Commissioner has an express audit function in relation to public sector agencies, credit providers and tax file number recipients, although the audit program has been cut back drastically in recent years due to resource constraints. The Victorian Privacy Commissioner also has an audit function which he has started to exercise in accordance with an Audit Manual published in 2004. All Privacy Commissioners are able to conduct special investigations and make special reports, although the parameters vary between jurisdictions.

[19] OFPC *Guidelines to the National Privacy Principles*, September 2001, Guidelines to NPP4.

[20] *E v Statutory Entity* [2003] VPrivCmr 5

could not have been reasonably anticipated. There are of course many other reasons, aside from privacy protection, why organisations put security precautions in place in relation to information. These include confidentiality of commercial matters and of government decision making processes, the need to ensure integrity of information for operational reasons, and concerns about physical security. The 'reasonable' security standard required by IPPs is the security necessary to protect personal information. The protection of commercial secrets or national security may justify higher security standards, but these would not seem to be the correct standards against which to judge whether an IPP has been breached.

Security objectives, whether for privacy protection or other reasons, are in constant tension with demands for accountability as expressed in Freedom of Information laws and corporate disclosure requirements, and in some cases with records/archives objectives. There are also clear tensions between convenience and security. User demands for ease and speed of access to information (including a person's rights of access to their own record) are not easily reconciled with security. The standard of what is 'reasonable' security must not be so strict as to be inconsistent with these other objectives being achieved, although the appropriate balance will vary.

The role of security standards

The dominance of other objectives has also led to much of the computer software currently in use for handling personal information being, in the view of many experts, fundamentally flawed from a security perspective.[21] Privacy regulators around the world have shown little appetite for 'taking on' the suppliers of commonly used hardware and software. In most cases[22] it would not be possible to do this through the mechanism of complaints or compliance audits, because the suppliers are not typically the holders of personal information held and processed using their products – any action would need to be against the users, who generally seem to assume that if a product is available and in widespread use then it must be OK to use it. There has been some useful discussion at the policy level, notably between some of the European privacy regulators and major software suppliers[23], but it is not clear whether there has yet been much 'privacy by design' as a result.

Despite these tensions, the other reasons for taking security measures has led to a major 'security' industry, well established long before privacy protection was added to the list of justifications. Because of the existence of this established expertise, Privacy regulators

---

[21] The vulnerabilities of, for example, Microsoft Windows, is well documented, and security concerns have been one of the foundations of the open-source software movement.

[22] The UK Data Protection Act 1998 does impose obligations on 'computer bureaux' as well as on users, but even this unusual feature does not reach equipment or software suppliers directly

[23] See for example various papers of the European Union's Article 29 Working Party at http://europa.eu.int/comm/justice_home/fsj/privacy/workinggroup/wpdocs/2006_en.htm and work by national Commissioners – some of which is listed at http://europa.eu.int/comm/justice_home/fsj/privacy/policy_papers/policy_papers_topic_en.htm

have often deferred to general standards and guidelines on security. The Australian Federal Privacy Commissioner's *Information Sheet: Security* (2001) includes a list of national and international security standards[24], as does the Victorian Privacy Commissioner's *Guidelines to the IPPs Part Two*, August 2002, and the three part NSW Information Security Guidelines[25].

The OECD's Information Security Guidelines[26], to which Australia states it adheres, are also relevant to interpreting security IPPs. They have been cited with approval by the NZ Privacy Commissioner, emphasising their focus on risk assessment and proportionality:

> "*Security levels, measures and costs should be appropriate and proportionate to the value of and degree of reliance on the information systems and the severity, probability and extent of potential harm, as the requirements of security vary depending on the particular information systems.*
>
> *When considering "reasonableness" in the security context, factors which may be relevant include:*
>
> • *the workability of the safeguards*
> • *the cost of the safeguards*
> • *the risks involved*
> • *the sensitivity of the information and*
> • *the other safeguards in place."*[27]

The OECD has continued its work on information security, most recently in the form of a joint workshop with APEC in Korea in September 2005[28].

For any profession or activity where such well-established security standards exist, Courts and Tribunals are likely to interpret what constitutes 'reasonable' steps in IPPs in light of such standards.

While the mass of security guidance available is potentially very valuable if used selectively, there is a risk in deferring entirely to established security industry standards. This is because many of them focus on only two of the three categories of risk – 'unauthorised access' and 'loss and corruption'. Traditional organisational security pays little attention to preventing or deterring 'unauthorised use by authorised personnel' – an

---

[24] Including the Australian Government's *Protective Security Manual* and Defence Signals Directorate Guidelines

[25] Most recently re-issued in 2003 – see http://www.oict.nsw.gov.au/content/2.3.16-Security-Pt1.asp

[26] Guidelines for the Security of Information Systems and Networks, 1992 http://www.oecd.org/dataoecd/16/22/15582260.pdf

[27] [2003] NZPrivCmr 22 (Cn28351)

[28] See http://www.oecd.org/dataoecd/1/23/35808919.pdf

internal threat. It is often assumed that if someone is entitled to access to information, what they do with the information is not a matter for physical or logical (computer) security. As noted above, all of the security IPPs are potentially broad enough to cover actions by 'authorised' persons as security breaches.

Inadvertent collection for security reasons

Clearly the need for security safeguards can be avoided altogether if personal information is not collected and held in the first place. While this is mainly the province of the separate collection principles, there may be instances where the initial collection is an unintended by-product of a security measure, or only takes place because of an over-zealous and unnecessary application of the security principle. It is incumbent on all organisations that are required to comply with privacy principles to apply the same criteria of justification and proportionality to collection of personal information for security reasons as to collection for mainstream operational purposes.

Examples of how this plays out in the context of personnel security are given below (p.11). Special consideration will need to be given to security where individuals are allowed to use 'common access' facilities. One example is a case in which the Victorian Privacy Commissioner required a public library to change the settings of the anti-virus software on its public access computers to avoid unnecessary copying and recording of files brought in on disk by users.[29]

'Need to know'

A key starting point for any security policy for personal information are the questions "Who needs access; for what purposes; in what circumstances, and under what conditions? The questions apply equally to internal and external (third party) access. The 'need to know' principle, while well known and accepted in military and national security arenas, has not traditionally been as familiar in mainstream government and business. Government secrecy and commercial confidentiality considerations have encouraged a 'need to know' mentality for some non-personal information (arguably not always in the public interest). But personal information, before the advent of privacy laws, generally fell into the category of a shared corporate resource, to be available to anyone within the organisation who might need it for whatever reason, even if the organisation was sensitive to the need to control external access.

One consequence of the introduction of privacy laws has been to focus the attention of organisations on the internal 'need to know' issue as a necessary part of compliance with the security principle. It has been a recurrent theme in complaints about breaches of that principle.[30]

---

[29] *W v Public Library* [2005] VPrivCmr 5

[30] Examples include *N v Local Council* [2004] VPrivCmr 8; *B v Australian Government Agency* [2006] PrivCmrA 2

One issue yet to be tested in case law is the appropriateness of supervisors or managers automatically having access to the same information as their subordinates. This practice is still common in many organisations, reflecting a traditional hierarchical view of management, but would often not survive an application of the 'need to know' principle. A variant of this issue is the questionable need for IT staff, notably systems administrators, to have access to all computerised data. The prevalence of this practice is probably attributable more to 'convenience' or perhaps rather a lazy assumption about what will be easiest for systems maintenance, without regard to the balancing obligation to protect individuals' privacy.

Access control minimum standards

Once an organisation has established who should and should not have access to personal information, it can move to consideration of the appropriate level of safeguards. While the appropriate level of security will of course depend partly on the risk, there are some minimum standards that should be obvious.

Reasonable physical access controls will include door locks, with appropriate key management. Technology now offers a range of options including biometric identification techniques. While some of these options are very powerful, whether they are reasonable in the circumstances will depend on other considerations including cost, and in the case of biometrics, employee privacy issues – further discussed under the 'Human Security' heading below.

Reasonable computer security should as a minimum include username and password/PIN controls for access to personal information. While it can be difficult to stop individuals using 'obvious' passwords or PINS, organisations could be held liable for making this too easy – many systems now require passwords/PINS to be of a minimum length and to contain prescribed features such as a mixture of alpha and numeric characters. Codes or numbers which are commonly known to third parties should not be used as passwords or PINS.[31] However there would appear to be limits to how far an organisation should be expected to go in preventing individuals from using 'guessable' passwords – The Privacy Commissioner of Canada rejected a complaint from an individual whose information had been accessed by a third party, finding that the respondents use of a user specified challenge/response safeguard was adequate, given that users had been expressly advised against using obvious questions and answers. The fact that the complainant had, contrary to this advice, specified her mother's maiden name was not the responsibility of the respondent.[32]

---

[31] See [2003] PrivCmrCan PIPEDA 146 – the Commissioner recommended the employer stop using the last four digits of employees Social Insurance Number (SIN) as the PIN for access to pay records – although surprisingly the security principle in PIPEDA was not cited. Also [2001] PrivCmrCan PIPEDA Case Summary #5, where the respondent agreed to change a password specification which was comprised of the individuals' telephone number and date of birth, in this case expressly to comply with the principle.

[32] [2005] PrivComrCan PIPEDA 315

There must also be reasonable controls to stop third parties finding out a customer's password or PIN. The Privacy Commissioner of Canada found that a telco had breached the security principle by allowing the PIN for a calling card to be retrieved by a 'last number recall' function[33], and the Hong Kong Commissioner found a mobile phone company to be in breach by allowing the use of back and history functions in Internet browsers to access password protected account details even after the user had closed the browser and gone offline.[34] This ruling suggests that the common practice of warning individuals using 'common access' facilities such as in Internet cafes to 'close the browser to prevent others seeing your information' may either be misleading or inadequate.

The role of logging and audit trails

Physical security, and logical access controls such as username/password combinations cannot control what use someone makes of information to which they are entitled. However, systems design features such as a requirement to record reasons for access, together with access logs or audit trails, are an important tool in deterring inappropriate uses. If users know that their access to information is recorded, and that they can be held accountable, then they are less likely to make unauthorised use of personal information.[35]

In *E v Financial Institution* [2003] PrivComrA 3, the Australian federal Privacy Commissioner found that the audit trail maintained by the respondent only recorded financial transactions, and not access to customers account information that did not involve an a transaction. The Commissioner concluded that as a result, the respondent "could provide only limited assurance that the information was protected from unauthorised access, misuse or disclosure." The financial institution in question "agreed to establish an enquiry audit trail on the mainframe computer where customer information is stored so that staff accesses to customers' personal information would be recorded regardless of whether a transaction is made on the account."

Organisations will of course want to know if cost considerations will be taken into account. In *FH v NSW Department of Corrective Services* [2003] NSWADT 72, when considering what were 'reasonable steps', the Tribunal was equivocal as to whether the estimated high cost of 'retro fitting' a logging facility on the Department's computer systems was a defence against an allegation of inadequate security, in breach of PPIPA s.12(c) – IPP 5. Despite finding that "the absence of arrangements to keep a record (a log) of who inside the administration is using the records, when and what for purpose" was a "significant continuing problem" the Tribunal appears to have accepted the respondents submission that installing such a facility would be prohibitively expensive.

---

[33] [2003] PrivCmrCan PIPEDA 254

[34] [2004] HKPrivCmr 4 (ar0304-6)

[35] Monitoring of employees' communications (as well as the extent of monitoring of their access to their employer's data, does of course raise separate privacy issues. The appropriate limits of employee or workplace privacy is one of the main current privacy debates.

Observing that the extent to which any shortcomings need to be addressed depends on both the risk of intrusion and the gravity of the consequences of intrusion, the Tribunal found "There is no basis for concluding that any further action should be taken at present by the Department to meet the applicant's concerns."

This is a particularly disappointing decision in that the Tribunal made no effort to test the respondent's assertions about the difficulty and cost of installing a logging facility, and does not appear to have made any comparison with the practice in other government agencies or private organizations. While it is understandable that there must be a practical limit on the amount an organization can be expected to pay for security, it cannot be satisfactory to leave the decision entirely to the organization, without any reference to contemporary standards.

Human security – training and enforcement

As well as logs and audit trails, the other main security measures that are effective against internal misuse fall into the category of personnel security, which encompasses both preventive measures such as appropriate (but not excessive) pre-employment vetting and training; and enforcement

Despite considerable education of users about confidentiality requirements and privacy laws, there continue to be abuses of access privileges. Since the early 1990s in Australia there have been a steady stream of reported cases (often concerning breaches of 'computer crime' laws[36]) where public servants have used information to which they had legitimate access for unauthorised purposes. In Australian government departments such as the Tax Office and Centrelink, where privacy laws are backed up by statutory secrecy provisions with criminal penalties, errant staff have been disciplined and in some cases prosecuted. Less satisfactory has been the response of Australian Police services to repeated instances of misuse by police officers and civilian employees – disciplinary action often seems to have been restricted to mild cautions – sending the wrong message about the gravity of the breaches.

The importance of training and internal communication of security measures was well illustrated by a case conciliated in 2003 by the Victorian Privacy Commissioner[37]. The complainant's new address was disclosed by an agency employee 'across the counter' despite corporate knowledge that the individual was at risk and had specifically requested that her new address be kept confidential. Indeed a separate request for the information on the same day by the same third person, presumably by more formal channels, had been correctly refused in accordance with the organisation's policy. This case highlights the problem of 'weak links' – in this instance an individual employee who was clearly not aware of the correct processes to ensure appropriate security. The outcome – a payment of $25,000 in compensation as well as a commitment to review procedures and

---

[36] Such as the *Crimes Act 1914* (Cth) Part VIIB

[37] *B v Victorian Government organisation* – [2003] VicCmr 2

communications – demonstrates again the potentially serious consequences of security breaches.

A similar reminder has been given by the NZ Complaints Review Tribunal in two cases involving unauthorised disclosure by a police officer.[38] In the absence of any evidence given by the Police service as to relevant security measures in the form of adequate training, the Tribunal found in both cases a prima facie breach of the security principle, ordering compensation of $10,000 in one case, while in the other there was an insufficient level of damage to amount to an interference with privacy.[39]

Organisations can obviously not be expected to guarantee compliance with instructions given to staff – individual employees will occasionally act wilfully and recklessly in contravention of clear instructions. This may result in the organisation being vicariously liable for the breach of another IPP by its staff member (see discussion of liability for disclosure below), but would not seem to be a breach of the security principle[40]. Where this happens, however, organisations could be expected to reinforce training and where appropriate to take disciplinary action in order to maintain a reasonable system of security. [41]

The issue of pre-employment screening or vetting involves a balance between protecting the privacy of 'customers' on the one hand, and not unduly intruding into the privacy of prospective employees on the other. In a health information case, the NZ Commissioner considered the normal practice of checking a medical practitioner's references, annual practising certificate and registration status to be 'reasonable' and therefore found no breach of the security rule of the Health Information Privacy Code.[42] Similarly the Privacy Commissioner of Canada found[43] that a nuclear power company was not acting unreasonably in requiring employees to consent to a security check (whether such a requirement would qualify as free and informed consent under the different laws is another issue). In another Canadian case, an employer's introduction of 'voiceprint' recognition technology as an access control device was held to be reasonable.[44]

---

[38] See *M v Police Commissioner*, [1999] NZ CRT 17/99, and *Proceedings Commissioner v Police Commissioner* [1999] NZ CRT 23/99

[39] The New Zealand Privacy Act has a two part test for an interference with privacy – there has to be not only a breach of a Principle but also significant detriment.

[40] See [2002] PrivCmrCan PIPEDA 100 – a bank's security was found to be adequate despite an unauthorised disclosure by an employee, in contravention of procedures and training

[41] See [2001] PrivCmrNZ 17 (Cn16005)

[42] [2001] PrivComrNZ 18 (Cn21451)

43 [2002] PrivCmrCan PIPEDA 65

[44] [2004] PrivCmrCan PIPEDA 281

Relationship between security and disclosure

Security breaches are often alleged as incidental to particular disclosures about which an individual complains. It will often be claimed that if a disclosure (or use) is found to be unauthorised or otherwise in breach of a use and/or disclosure principle, then it follows that there must have been a security breach as well. That this does not automatically follow is clear from the 'reasonable steps' qualification to the principles. No-one expects security to be absolute – even the best precautions are likely to be vulnerable to both human error and deliberate circumvention. Computer security is known to be a constant battleground between the clever hackers/crackers on the one hand and the security experts (often reformed hackers) on the other.

The prospect of inappropriate disclosures not necessarily involving a security breach is illustrated by AAB Appeal 4/00 in which the Hong Kong Administrative Appeals Board dismissed a complaint that newspaper publication of the complainant's address, endangering him, was a breach of the security principle in the Hong Kong Ordinance[45]. It considered that only the disclosure principle was at issue.

In contrast, the only formal determination by the Australian federal Privacy Commissioner to deal with the security principle found a breach of IPP4 apparently 'automatically' as a result of an unauthorised disclosure of details of an Army discharge.[46] No other reason is given for the finding, which was not contested[47] . The case did however highlight, relatively early in the operation of the federal Act, the potential for damage to result from inadequate security – the complainant was sacked by his new employer as a direct result of the disclosure. The Commissioner awarded compensation of $5000 – half for lost earnings and half for embarrassment.

It would seem reasonable to suggest that a disclosure will only involve a breach of the security principle if it could have been prevented had better security procedures been in place. The consequences of the disclosure will then be consequences of the associated security breach, and may result in compensation such as in the above example.

Breaches of the security principle by an organisation may also involve a breach of computer crime laws or similar crimes by the person whose actions have demonstrated the security weaknesses. A hacker may have breached computer crime laws (and be of inadequate means for a claim for compensation), but the organisation that has been hacked may have breached the security principle and will be a much better target for a compensation claim.

---

[45] See http://www.pco.org.hk/english/ordinance/ordfull.html - Data Protection Principle 4 requires 'practicable steps' to guard against the same risks as the similar principles in Australasian laws.

[46] *A v Dept of Defence* – [1993] PrivCmrACD 1

[47] The agency concerned wished to make an ex gratia payment but considered its legislation did not allow this.

Liability for disclosure

Another important aspect of the relationship between the security and disclosure principles is that, while organisations can eliminate security liability by taking reasonable steps, when a breach does occur which results in disclosure it seems at first sight that the disclosure principles (e.g. NPP 2 in the AusPA) imposes an absolute liability despite reasonable security procedures. Usually, this will be the case where unauthorised disclosure occurs, and can be justified on the grounds that the organisation is better able to bear the loss than the individual. In other words, no matter what steps organisations take to improve security, they cannot remove disclosure liability (although a 2004 NSW Tribunal case has cast doubt on this at least under PPIPA[48]).

However there is one gloss on this, in that the disclosure principle only applies when it is the organisation that discloses the information. Usually, where this happens there will also be a breach of the security principle, but in rare cases this could occur despite normally adequate security (e.g. if a completely unknown technical flaw in software causes an organisation to publish customer information on its website). In such cases it is the organisation that has published the information and is liable.

However, in the case of third party hackers extracting information from a site, it is hard to see that it is the organisation that is 'disclosing' the information. If it takes a wilful criminal breach of normally reasonable security then perhaps the customer will have to bear the loss. This will also be a rare event, because hacking will normally exploit an inadequacy in security.

The position will sometimes be different in New Zealand, because s126(4) NZ PA provides that employers will not be liable for breaches of any of the principles by employees where they took 'such steps as were reasonably practicable to prevent the employee from doing that act'.

Standing for security complaints

Another aspect of the relationship between security and disclosure is the question of ‘standing’ to bring a complaint.

As an example, the AusPA provides that “An act or practice is only an ‘interference with the privacy of an individual if it breaches the NPPs (or a Code) *in relation to personal information that relates to the individual”* (s.13A) (emphasis added).

The question that arises is whether an individual can complain about a breach of the security principle without having evidence of any personal information *about them* having been lost, disclosed inappropriately etc? Or even without evidence of *any* actual loss, disclosure etc? A complainant would clearly have to be able to establish that the

---

[48] In *NS v Commissioner, Department of Corrective Services* [2004] NSWADT 45, the Tribunal found that the Department was not responsible for a serious unauthorised disclosure (of criminal history) by an employee who had clearly ignored what were held to be adequate security warnings.

organisation in question held information about them, but is it sufficient to establish that their personal information has been put at risk by inadequate security?

The answer to this question will depend on the wording of the individual laws, outside the principles themselves, and is a matter for consideration elsewhere. However, it is interesting to note that in a Canadian Case, the Commissioner concluded:

> "…that no improper disclosure of the complainant's personal information had occurred. He determined that the company had not by any failure on its part enabled a third party to gain access to the complainant's personal information. Since no breach of security had been demonstrated, he could not conclude that the company had failed to institute appropriate safeguards."[49]

Communications security

Security measures must obviously apply to communication or transmission of personal information as well as to its storage. With computerised data even more than paper records, the distinction is often blurred – transmission is inherent in storage and routine use even within a single workstation as well as in transfer or disclosure between offices or to third parties.

A comprehensive security strategy will consider all the points of vulnerability – particularly to unauthorised access, and put in place appropriate controls. Where transmission of personal information is by electronic means, a key decision will be when to employ encryption.

While belatedly drawing attention to encryption as a tool[50], Privacy regulators have generally been reticent about when encryption should be used for the transmission of personal information, partly because of concerns about cost and partly because so many information technology systems have been designed and implemented with relatively low levels of security, making any attempt to enforce an encryption requirement across the board unrealistic.

Regulators are starting to give guidance about when encryption might be appropriate. In 2004 Website Guidelines, the Victorian Commissioner implies that encryption might be necessary for financial data.[51] And in a Report of investigation into a major unauthorised disclosure incident, the Commissioner has recommended the use of encryption for

---

[49] [2002] PrivCmrCan PIPEDA 41

[50] See Australian Privacy Commissioner, *Guidelines for Federal and ACT Government Websites*, May 1999, preamble to Guideline 3; Victorian Privacy Commissioner, *Website Privacy: Guidelines for the Victorian Public Service*, May 2004, pp 17-18. Note that the earlier general Guidelines from both Commissioners (see footnote 7) do not even mention encryption expressly.

[51] Victorian Privacy Commissioner, *Website Privacy: Guidelines for the Victorian Public Service*, May 2004, p18

information exchanges between the Office of Police Integrity, and other bodies including Victoria Police.[52]

An understandable focus on IT security should not overlook that one of the most common causes of security breaches is carelessness in delivering personal information by more traditional means. Examples of careless practice that have been highlighted in reported cases include:

- Failure to seal envelopes containing sensitive information, so that intermediaries (couriers, neighbours, other family members) are able to access and read the contents[53].
- Putting material about one person in envelopes addressed to another person[54]
- Faxing personal information either to the wrong fax machine[55], or to machines in common areas without taking steps to ensure the intended recipient is on hand to collect the pages[56].
- Printing of sensitive personal information on envelopes[57], or on correspondence visible through envelope windows[58] (Note however that appropriate use of Window envelopes has been recommended by the NZ Commissioner as a security precaution.[59])

It is however not unreasonable for organisations to rely on postal services, even though they are not faultless, and that incorrect delivery can sometimes lead to unauthorised

---

[52] Report 01-06 Jenny's case: Report of an Investigation into the Office of Police Integrity pursuant to Part 6 of the Information Privacy Act 2000, February 2006, Section 10 – Recommendation 8. The Commissioner also issued the first compliance notice under the IPA, requiring an independent security audit of, amongst other things, the "management of flows between OPI and Victoria Police of electronic data …"

[53] See HKPrivCmr ar9798-10; [2002] HKPrivCmr 7 (ar0203-6), and [2002] HKPrivCmr 8 (ar0203-7). Also [2003] PrivCmrCan PIPEDA 154 in which the Commissioner held that a bank should institute manual checks to ensure that envelopes containing sensitive personal information are sealed.

[54] See [2002] PrivCmrCan PIPEDA Case Summary 28 – the bank in question agreed to institute a 'double verification' process in its mailroom

[55] See [2001] HKPrivCmr 5; ar0102-5; [2005] PrivCmrA 2.

[56] See M v Cth Agency [2003] PrivComrA 1; [1999] NZPrivCmr 11 (Cn13518); [2003] PrivCmrCan PIPEDA 226; [2005] PrivCmrCan PIPEDA 317 .

[57] See [1998] HKPrivCmr 12 (ar9798-17)

[58] Two cases involving the risk of disclosure through use of window envelopes were settled during the course of investigation by the Privacy Commissioner of Canada in 2004 - http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040706_e.asp

[59] See [1998] PrivCmrNZ 2 (Cn2448) – the use of window envelopes eliminates the need to match contents to envelopes, reducing the type of risk highlighted in the Canadian case cited at footnote 26.

disclosure. The Privacy Commissioner of Canada found that a bank's reliance on first class mail for despatch of credit cards was not unreasonable – the complainant had felt that they should have used registered mail but the Commissioner disagreed[60]. A New Zealand case suggests that even wrongly addressed mail need not necessarily imply a failure of security.[61]

Apparently inconsistent interpretations can often be explained by the detailed circumstances of the cases. The NZ Commissioner rejected a complaint about the use of courier for delivery, despite the fact that documents had been lost, finding that the use of a recognised courier service was in fact a reasonable security precaution (for delivery of credit file information), and that the lack of a requirement for signature on receipt was not unreasonable given that reports were usually sent my regular mail[62]. In a recent Australian case, the Commissioner found that reliance on the standard conditions of carriage by a courier company, which did not include a requirement for signature on receipt, was inadequate for the information in question (Superannuation Fund board papers) and conciliated a settlement with $3,500 compensation and an agreement to require signature on receipt in future[63]. However, in the latter case the documents in question had ended up scattered on a public footpath, with the potential for public disclosure, whereas in the NZ case they had simply been lost. It is to be hoped however that the difference in finding related more to the sensitivity of the information – the actual consequences of the disclosure, while relevant to the remedy (such as the amount of compensation) should not affect the finding of a breach i.e. whether the use of the courier without signature on receipt was 'reasonable'.

Careless disclosure – other examples

Outside the context of personal information 'in transit', careless disclosure can also arise from:

- procedures for sign-in or registration which unnecessarily reveal information about previous registrants[64];
- failure to delete the details of third party individuals from documents provided under Freedom of Information or other 'access' legislation (this arises with any release of information)[65];

---

[60] See [2002] PrivCmrCan PIPEDA 43

[61] [1998] PrivCmrNZ 15 (Cn14982)

[62] [1998] PrivCmrNZ 8 (CN6983)

[63] See *J v Superannuation Provider* [2005] PrivComrA 7

[64] See [1998] HKPrivCmr 4 (ar9798-16); [2005] PrivCmrCan PIPEDA 304

[65] See B v Victorian Government organisation – [2003] VicCmr 2 and NV v Randwick City Council [2005] NSWADT 45

- use of 'real' personal information in training or in publications – such as when illustrating a point with a case study[66], or in providing 'test' databases for training or demonstrations[67], and

- failure to ensure security for personal information 'out of office' or 'out of hours' – the Hong Kong Privacy Commissioner has served an enforcement notice[68] on a bank to implement appropriate policies and practices[69].

- failure to provide reasonably confidential facilities for discussion with clients[70].

- the filing of facsimiles on thermal paper which fade over time[71] (an example of inadequate security in the widest sense leading to loss of personal information).

Another common security breach arises when documents containing personal information are accidentally mislaid or disposed of insecurely. Personal information often resides on computers which are lost or stolen – in 1995 sensitive personal information was contained on the hard drives stolen from the ACT Department of Education and Training. The Privacy Commissioner's investigation concluded that while there was no evidence of anyone having accessed the information (the thieves were more likely to be interested in the value of the hardware), there had been a number of security failures. His report recommended improved building and computer security, a review of the need to keep sensitive information on local hard drives, and enhanced staff training.[72]

Obligations when contracting services

Another recommendation of the Australian Federal Commissioner's report into the theft from the ACT Department, mentioned above, which is of general application, was the need for agencies to ensure that contracts with IT service providers contain appropriate clauses concerning privacy obligations. Given the prevalence of outsourcing of IT functions in particular, agencies need to accept that they cannot escape responsibility for

---

[66] See [2002] NZPrivCmr 2 (Cn26280)

[67] This has been a common audit finding – see for example Federal Privacy Commissioner Ninth Annual Report 1996-97 p.95

[68] Under s.50 of the HK Personal Data (Privacy) Ordinance. Note that the Victorian Privacy Commissioner has a similar 'compliance notice' power (IPA s.44), see footnote 44

[69] HKPCO Newsletter August 2004 - http://www.pco.org.hk/english/publications/newsletter_issue13.html and [2004] HKPrivCmr 3 (ar0304-7) .

[70] See [1995] PrivCmrNZ Case Note 2594 – no breach in the particular case but the agency agreed to instal a private office.

[71] Federal Privacy Commissioner Ninth Annual Report 1996-97 p.95 – common audit findings.

[72] Federal Privacy Commissioner Ninth Annual Report 1996-97 p.124

privacy compliance just because the actual privacy breach was committed by a contractor. Some of the Security principles contain an express reminder of this – requiring agencies to ensure that reasonable steps are taken to prevent security breaches by contractors.[73] Some of the laws place responsibility more generally on agencies for any actions of contractors[74], although under some laws contractors can also be investigated and held directly liable for breaches.[75]

The New Zealand Privacy Commissioner has found that a failure by a debt collection agency to ensure that sub-contracted process servers were aware of their privacy obligations led to an inappropriate disclosure, and that the failure constituted a breach of the NZ security principle IPP5.[76]

Programming errors and multiple breaches

There have been several well publicised incidents of mass mail-out errors by Australian federal government agencies, some of which have led to major investigations by the Federal Privacy Commissioner. In his reports, the Commissioner found that the agencies had not taken adequate steps to prevent the sort of systems errors that led to the mismatching of personal details such that letters intended for one person were sent by mistake to another client.[77] It would not however be reasonable to expect a guarantee of 100% error free automated mailing – the NZ Commissioner found that a one-off enclosure of multiple letters in one envelope had unfortunately occurred despite generally adequate security[78].

Although these instances of bulk/multiple breaches would be fertile ground for representative actions under the federal Privacy Act, no such actions have yet been brought in this context.

Access control must be managed

It is clearly not sufficient to have security measures in place if they are not implemented. In *L v Commonwealth Agency* [2003] PrivComrA 10, the agency failed to ask for a password that had been issued to a client, and as a result disclosed personal information

---

[73] PA s.14, IPP 4(b); PPIPA s.12(d).

[74] PA s.8(1); IPA s.9(1)(j) and s.17 (an agency can expressly transfer the obligations by contract); PPIPA s.4(4)(b).

[75] E.g. *Privacy Act 1988.*

[76] [1998] PrivCmrNZ 6 (Cn2663)

[77] Errors of this nature were made by the Australian Taxation Office, the then Department of Social Security and the Department of Veterans Affairs in the mid 1990s, by the Department of Education and Training in 1995-96 (Privacy Commissioner Eighth Annual Report 1995-96 p.114) and by a mailing house acting on behalf of a credit union in September 1996 (Ninth AR p 100)

[78] See [2003] NZPrivCmr 22 (Cn28351)

about him to his ex-wife. The Commissioner found the agency in breach of IPP4 and the agency agreed to update its computer system to prompt for passwords.

Another case handled by the federal Commissioner[79] raised the question of whether an Internet Service Provider (ISP) had taken reasonable steps to implement password security – the complainant alleged that his estranged wife had been able to access his Internet account after several attempts despite his having changed the password. Unfortunately the Commissioner declined to investigate on the grounds that the complainant had apparently not taken the matter up first with the ISP in question. This case could have thrown useful light on what standards an ISP will be required to meet in relation to controlling access to customers' accounts. A subsequent case did offer some guidance – the failure by an ISP to correctly and consistently follow security procedures in allowing an unauthorised third party to reset a password and gain access to account details, amounted to breach of NPP 4.1 leading to breach of NPP2.1[80].

Most systems administrators would be aware of the need for regular password changes, and for revocation or change to access privileges for staff who leave or have changed function, but audits commonly find that these disciplines are not enforced. Similar obligations apply to management of physical access – for example the need to supervise after hours access by contractors, and to change key pad combinations and retrieve keys from departing staff.[81]

Guidance from audit findings

In those privacy jurisdictions which provide for audits, audit findings provide another source of guidance as to what regulators consider to be 'reasonable' security safeguards. In the early to mid 1990s the Australian Federal Privacy Commissioner either undertook or commissioned a large number of audits – of Commonwealth agencies, credit providers and credit reference agencies and of financial institutions' compliance with the tax file number guidelines[82.]

Resource constraints have meant a marked reduction in the number of audits conducted in recent years and the audit power was not extended to the private sector generally when it became subject to the National Privacy Principles from 2001. Nevertheless the individual audit reports that have been published, and the more generalised findings that now appear in the Annual Reports, do continue to provide further insight into the Commissioner's interpretation of the security principle – most audits have found at least some aspects of security that require attention.

---

[79] *N v Internet Service Provider* [2004] PrivCmrA 10.

[80] *R v Internet Service Provider* [2005] PrivCmrA 17 – confidential settlement

[81] Federal Privacy Commissioner Ninth Annual Report 1996-97 p.95 – common audit findings.

[82] These were the three jurisdictions in the Australian federal *Privacy Act 1988* until the addition of the private sector NPPs in 2000.

The Commissioner's audit of federal government websites in 2001[83] found that 47.6% of websites audited collected personal information that is transmitted over the Internet. However, less than half of the sites that collect personal information in this way warn users of the risks of transmitting data over the Internet. A very small number of all sites (3.6%) provide online purchasing and 2.8% provide secure facilities for doing so. The Commissioner concluded:

> "It is also a matter of concern that in the areas of collection and security, levels of compliance with the guidelines remain inadequate."

It is to be expected that there would now be significantly more personal information transactions through Commonwealth agency websites, and attention to security has hopefully improved.

More recently, the Victorian Commissioner has started to exercise his audit power under the IPA. During 2005, 62 websites were audited, and comparison made with the results of an earlier (2003) audit.[84] One of the 'tests' performed was to answer the question: "Does the site provide secure facilities for the transmission of personal information?" (Test 2(d))

Results were 15% yes for all (up from 6%); 6% yes for some (down from 12%); 39% none (down from 51%), and 40% no online transactions requiring pi (up from 31%)

The Commissioner commented:

> "This was another disappointing result, particularly given that the IPP 4 requirement is 'reasonable steps' rather than a more absolute measure."

He recommended: "Organisations subject to the IPA should provide users with secure online facilities where personal information is subject to transmission" (Recommendation 8).

Conclusion

Privacy case law in a variety of jurisdictions is gradually throwing some light on what constitute the 'reasonable security measures' required by privacy laws, supporting in more authoritative way the other guidance available in guidelines and audit reports. Research for this article has only looked at a selection of the case law available, and further guidance may be available from other cases.

As the body of case law builds up and is analysed and summarised[85], organisations can expect to obtain a clearer view of their obligations, both generally and in a variety of

---

[83] Privacy Compliance Audit: Commonwealth Government Web Sites, August 2001 http://www.privacy.gov.au/publications/wsr01.html#_Toc521734767

[84] Privacy Victoria, Audit of Public Sector Websites – Report October 2005

[85] Not least by the Interpreting Privacy Principles project at UNSW – see http://www.cyberlawcentre.org/ipp/

specific circumstances. Complainants and their representatives will be able to make a more realistic assessment of their claims for redress. Privacy regulators themselves will be able to compare interpretations, hopefully resulting in more consistent and predictable enforcement.