DRAFT

Working Paper No 1

Interpreting the Security Principle

v.6 March 2007

Nigel Waters, Graham Greenleaf and Paul Roth

Respectively Principal Researcher, Chief Investigator and Partner Investigator on the Interpreting Privacy Principles Project, Cyberspace Law and Policy Centre, University of New South Wales, http://www.cyberlawcentre.org/ipp/

This paper has its origins in 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

A subsequent version was presented to a project Symposium *Interpreting Privacy Principles: Chaos or Consistency?* held in Sydney on 17 May 2006

We acknowledge the assistance of Abi Paramaguru, Research Assistant on the iPP project

DRAFT

Contents

Introduction

This paper is part of a series that explores the way in which information privacy principles have been enacted, and are being interpreted, in various jurisdictions. While the emphasis of the series is on Australian privacy laws, comparisons are made with other jurisdictions, particularly those in the Asia Pacific Region with similar laws – notably New Zealand, Hong Kong and Canada, but also, where appropriate, with the rich European experience of Data Protection law. The form and meaning of the principle are referenced back to their common origins in seminal international instruments, and relationships to new instruments, such as the APEC Privacy Framework, are also considered. The paper, like others in the series, concludes by offering a model for an 'ideal' security principle, for consideration in law reform.

Security in context

All privacy laws contain a security principle, which applies to personal information held by an organisation.[1] 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.

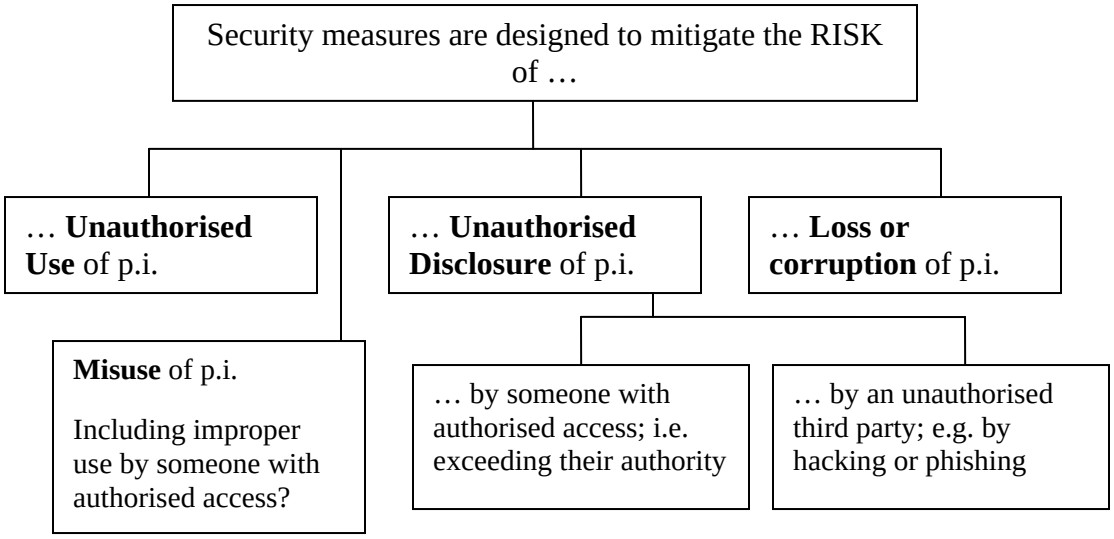

Figure 1

[1] There are clearly important questions about when personal information is 'held' for the purposes of privacy laws, but these will be explored in other papers in this series. For the purposes of this paper, we assume that that threshold question has been answered and that security obligations do apply to personal information.

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.[2]

The security principle in privacy laws interacts closely with other principles. The risks that security measures must protect against include inappropriate use and disclosure - which are principles in their own right - and also against corruption (covered by data quality principles). Poor security by one party can also contribute to inappropriate collection by another party, potentially in breach of collection principles. Some of these relationships are addressed in more detail later in this paper.

International privacy instruments

All the main international privacy instruments contain a security principle.

> "Appropriate security measures shall be taken for the protection of personal data stored in automated data files against accidental or unauthorised destruction or accidental loss as well as against unauthorised access, alteration or dissemination. (Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Convention No 1981, Article 7[3])

> "Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data." (OECD Guidelines governing the protection of privacy and transborder flows of personal data, 1980, Principle 11[4])

> "…the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing. … Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security

---

[2] [1995] PrivCmrNZ Case Note 3984

[3] http://www.worldlii.org/int/other/PrivLRes/1981/1.html (4-12-06)

[4] http://www.worldlii.org/int/other/PrivLRes/1980/1.html (4-12-06). The OECD subsequently (1992) issued additional Guidelines specifically on Security of Information Systems, http://www.oecd.org/document/19/0,2340,en_2649_37441_1815059_1_1_1_37441,00.html revised in 2002 – see http://www.worldlii.org/int/other/PrivLRes/2002/1.html (4-12-06)

> appropriate to the risks represented by the processing and the nature of the data to be protected." (EU Directive 95/46, Article 17.1[5])
>
> "Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment." (APEC Privacy Framework 2005, Principle VII[6])

Explanatory material attached to some of these instruments usefully outline the intended scope of the principles. For example:

> "Security and privacy issues are not identical. However, limitations on data use and disclosure should be reinforced by security safeguards. Such safeguards include physical measures (locked doors and identification cards, for instance), organisational measures (such as authority levels with regard to access to data) and, particularly in computer systems, informational measures (such as enciphering and threat monitoring of unusual activities and responses to them). It should be emphasised that the category of organisational measures includes obligations for data processing personnel to maintain confidentiality. [The security safeguards principle] has a broad coverage. The cases mentioned in the provision are to some extent overlapping (eg access/disclosure). 'Loss' of data encompasses such cases as accidental erasure of data, destruction of data storage media (and thus destruction of data) and theft of data storage media. 'Modified' should be construed to cover unauthorised input of data, and 'use' to cover unauthorised copying."[7]

---

[5] http://www.worldlii.org/int/other/PrivLRes/1995/1.html (4-12-06)

[6] http://www.worldlii.org/int/other/PrivLRes/2005/4.html (5-12-06)

[7] *Appendix to the OECD Privacy Guidelines: Explanatory Memorandum* (Paris, 1980), para 56 – see http://www.oecd.org/document/18/0,2340,en_2649_37441_1815186_1_1_1_37441,00.html

Domestic privacy regulation

The security principles in most Australasian privacy laws, codes and other domestic instruments reflect those in the international instruments[8] and are all very similar in effect though there are superficial differences. The first to be enacted – 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[9] s.14).

The NSW and NZ laws contain an almost identical principle (NSW PPIPA[10] s.12(c) – IPP5; NZPA[11] 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[12] IPP 4.1), in the Northern Territory *Information Act* (NT IA[13] IPP 4.1), and in the Tasmanian *Personal Information Protection Act 2004* (TPIPA[14] IPP 4.1).

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[15]. These principles generally deal with additional

---

[8] Such as the OECD Guidelines (1980) and Council of Europe Convention (1981), and also in subsequent international instruments including the European Union Directive (1995) and the recent APEC Privacy Framework (2004).

[9] *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

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

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

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

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

[14] *Personal Information Protection Act 2004 (Tas)* – TPIPA herein

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

notification and consent requirements and are silent on security. But it remains implicit[16] 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[17] 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.

'Reasonable steps' – sources of interpretation

A common feature of security principles in privacy laws is the qualification that the obligation is only to take 'reasonable' or 'reasonably practicable'[18] steps – either expressly or implicitly related to the particular circumstances. The origin of these qualifications is to be found in clause 16 of the OECD Security Guidelines:

The concept of proportionality is expressly included in APEC security principle cited above, and in the 2002 OECD Security Guidelines:

> "Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation's systems and networks." [19]

Informal Guidance

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[20] emphasise the need for a risk assessment. So too do the NSW government security guidelines which also suggest a 'baseline' level of

---

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

[17] *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)*

[18] The Council of Europe Convention already cited, and security principles in the UK Data Protection Act 1998 and the US Federal Privacy Act 1974 both use the term 'appropriate' but this implies a similar concept of 'proportionality'.

[19] Guidelines for the Security of Information Systems and Networks 2002Principle 7 - security design and implementation - http://www.worldlii.org/int/other/PrivLRes/2002/1.html

.

[20] 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* edition .02 September 2006, pp 90-111.

precautions, with extra measures to deal with particular risks[21]. 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[22].

Jurisprudence

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

Privacy jurisprudence has been slow to develop in Australia. Most of the Commissioners are now publishing 'casenotes', summarising the outcome of conciliated complaints or own-motion investigations. However, casenotes are not binding and cannot be used as legal precedent – they carry no more weight than the guidelines.

After 17 years there have still been only eight formal complaint Determinations by the Federal Privacy Commissioner, and a mere handful of court decisions involving the *Privacy Act 1988 (Cwth)* – mostly dealing with aspects other than the principles – as there is no merits review of the Commissioner's Determinations[23].

The NSW law has been litigated more intensively, with around one hundred decisions of the Administrative Decisions Tribunal (ADT) on the *Privacy and Personal Information Protection Act 1998 (NSW)*, and several Supreme Court decisions on appeal. The Victorian Civil and Administrative Tribunal (VCAT) has also started to make decisions under the *Information Privacy Act 2000 (Vic)*. Some hundreds of formal decisions are however now available from the New Zealand, Hong Kong, and Canadian jurisdictions.

Between all the jurisdictions, there are now a number 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

---

[21] http://www.oict.nsw.gov.au/pages.asp?CAT=764&ID=793 (5-12-06)

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

[23] Other than on the quantum of compensation – one case to date has been taken, resulting in the Administrative Appeals Tribunal (AAT) increasing the amount of compensation awarded from zero to $8000 - Rummery and Federal Privacy Commissioner and Anor [2004] AATA 1221.

in the reports of special investigations and audits conducted by those Commissioners who have those functions[24]. 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[25]: 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[26]. The Commissioner handled a similar case in 2006, which involved unintended disclosure of personal information on the web about entrants to a competition run by a government department.[27] The resolution of this case also required the co-operation of a major search engine operator These cases raise important issues of historical records/archives, which will be canvassed further in subsequent analysis of the retention and correction principles.

---

[24] 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.

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

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

[27] Complainant AD & Others v The Department [2006] VPrivCmr 5

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. There will also be occasional lapses and accidents, which will not necessarily mean that security measures were not adequate – examples are given later in this paper. Security obligations are not absolute, and need to be balanced against other interests and obligations**.**

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 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.[28] Privacy regulators around the world have shown little appetite for 'taking on' the suppliers of commonly used hardware and software. In most cases[29] 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

[28] 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.

[29] 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

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[30], 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 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[31], as do the Victorian Privacy Commissioner's IPP Guidelines[32], and the three part NSW Information Security Guidelines[33]. National and international standards on generic risk management[34] are also often cited, but care should be taken not to assume that such generic standards will necessarily be judged as adequate in the specific context of security of personal information.

The OECD's Information Security Guidelines, already cited above, are also relevant to interpreting security IPPs. The first 'edition' of the Guidelines[35] have been noted with approval by the NZ Privacy Commissioner, emphasising their focus on risk assessment and proportionality, and their identification of relevant factors:

> "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

---

[30] 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 (5-12-06) 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 (5-12-06)

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

[32] Office of the Victorian Privacy Commissioner, Guidelines to the Information Privacy Principles, September 2006, footnote 175

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

[34] Such as AS/NZS4360 2004 – Risk Management.

[35] Guidelines for the Security of Information Systems and Networks, 1992 - http://www.oecd.org/document/19/0,2340,en_2649_37441_1815059_1_1_1_37441,00.html

• the sensitivity of the information and
• the other safeguards in place."[36]

The OECD's revised 2002 Guidelines expressly address the issue of risk assessment:

> ***"Participants should conduct risk assessments.***
>
> Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others."[37]

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[38].

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 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.

Security obligations in other legislation

Many other laws include information security obligations, either expressly or implicitly. Public sector agencies are typically subject to secrecy provisions in the statutes they administer, and these contain at least implicitly an obligation to implement appropriate security measures. Public sector auditors regularly comment on security matters both in

---

[36] [2003] NZPrivCmr 22 (Case Note 28351)

[37] Principle 6 – Risk Assessment – at http://www.worldlii.org/int/other/PrivLRes/2002/1.html

[38] http://www.oecd.org/dataoecd/1/23/35808919.pdf (21-2-07)

performance audits and in relation to traditional financial accountability.[39] Accounting and corporate governance standards indirectly require appropriate security, and sectoral legislation applying to many private sector businesses can also include either direct or indirect requirements to safeguard information – and while typically personal information is not singled out, it is covered by more general requirements.

Responsibility for enforcement of security requirements in other laws lies with a range of different regulators, but it is clear that some of these take security breaches much more seriously than most Privacy Commissioners. In a recent case in the UK, the Financial Services Authority (FSA) fined the Nationwide Building Society nearly one million pounds for losing a laptop that contained customer data. The FSA investigation found that the building society did not have adequate information security procedures and controls in place. It was found to be in breach of the FSA Principle 3, which states that a firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems. A further reason given by the FSA was that the firm "failed to implement adequate training and monitoring to ensure that its information security procedures were disseminated and understood by staff."[40]The penalty imposed in this case stands in stark contrast with the remedies and sanctions available under the UK Data Protection Act 1998, the security principle of which is much clearer than the FSA Principle 3.

As long ago as 2004, the FSA was calling for better information security to combat fraud and other financial crime.

In Australia, financial sector regulators have issued specific advice on security. From the prudential regulator APRA in 2004:

> "19. The technical resources that a [licensed superannuation fund trustee] is required to maintain, or have access to, at an adequate level include, but are not limited to: …
>
> (b)adequate systems and resources to ensure protection, security and privacy of confidential, personal and sensitive material; and …

---

[39] The Audit Office of New South Wales, New South Wales Auditor General Reports, Financial Audits, "Compliance Review of Security of Electronic Information", Volume 4, 2004 <http://www.audit.nsw.gov.au/publications/reports/financial/2004/vol4/CompReview%20Security%20of%20Information%20Report.pdf> , Tasmanian Audit Office, "Auditor-General Special Report No. 60: Building Security and Contracts Appointing Global Value Management", May 2006 <http://www.audit.tas.gov.au/publications/reports/specialreport/pdfs/specialreport60.pdf>, Auditor-General Victoria, "Auditor General's Report – Results of financial statement audits for agencies with other than 30 June 2004 balance dates, and other audits", May 2005, see section 6, 'Management of internet security by local governments' at <http://www.audit.vic.gov.au/reports_mp_psa/psa1206.html > and Office of the Auditor General of Canada, 2005 Status Report, "Chapter 1: Information Technology Security" <http://www.oag-bvg.gc.ca/domino/reports.nsf/html/20050201ce.html>

[40] Report in Privacy Laws & Business International E-News Issue 54, 16 February 2007

(d) evidence of the inclusion in the risk management framework of processes to ensure security of records and compliance with statutory privacy laws." (pp. 8-9) (emphasis added)[41]

APRA also advise that security should be specifically addressed in any 'outsourcing' contracts. [42]

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.[43]

---

[41] APRA Guidance Notes and Circulars, July 2004, Superannuation guidance note SGN 140.1 – http://www.apra.gov.au/Superannuation/upload/SGN-140-1-Adequacy-of-resources.pdf

[42] APRA Guidance Notes and Circulars, July 2004, Superannuation guidance note SGN 130.1 - http://www.apra.gov.au/Superannuation/upload/SGN-130-1-Outsourcing.pdf, and Prudential Standard APS 231- Outsourcing - http://www.apra.gov.au/policy/final_adi_standards/APS231.pdf

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

Special Protection for Sensitive Information?

There do not appear to have been any cases involving the separate health privacy jurisdictions to date that add to our knowledge of the specific security measures that might be considered necessary when handling health information.

Another 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.[44] Canadian cases have highlighted the need for special protection for the Social Insurance Number (SIN)[45] and similar cases can be expected in those Australia jurisdictions that require special protection for government identifiers[46].

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 cheques out with account statements.[47] 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.

'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

---

[44] [1997] PrivCmrNZ 12 (Case Note 10668) and [1994] PrivCmrNZ (Case Note) 0189

[45] [2002] PrivCmrCan PIPEDA 69 , 2002 CanLII 42335 (P.C.C.); [2003] PrivCmrCan PIPEDA *146*, 2003 CanLII 38598 (P.C.C.)

[46] AusPA NPP7, and IPA IPP7

[47] [2005] PrivCmrCan PIPEDA 299 *Thief cashes convenience cheque on cancelled credit card account*, 2005 CanLII 27661 (P.C.C.)

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.[48]

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, to contain prescribed features such as a mixture of alpha and numeric characters, and to be changed periodically[49]. Codes or numbers which are commonly known to third parties should not

---

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

[49] [2006] PrivCmrA 8 – the Commissioner was satisfied that the retail company's database was only accessible to a small number of people within the company, that the database was password protected and that passwords were routinely changed as a security measure.

be used as passwords or PINS.[50] 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.[51]

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[52], 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.[53] 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.

---

[50] [2003] PrivCmrCan PIPEDA 146, 2003 CanLII 38598 (P.C.C.) – 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, 2001 CanLII 21542 (P.C.C.), 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.

[51] [2005] PrivComrCan PIPEDA 315 *Web-centred company's safeguards and handling of access request and privacy complaint questioned*, 2005 CanLII 37355 (P.C.C.)

[52] [2003] PrivCmrCan PIPEDA 254 , 2003 CanLII 1100 (P.C.C.)

[53] [2004] HKPrivCmr 4 (ar0304-6)

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.[54]

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." The Commissioner has re-inforced the need for an audit trail in a more recent case.[55]

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. 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.

---

[54] 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.

[55] [2006] PrivCmrA 13

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[56]) 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.[57] 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[58]. 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 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.[59] 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,

---

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

[57] See for instance "Welfare workers axed for spying", The Australian, 23 August 2006, p. 1

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

[59] *K v Police Commissioner* (unreported, Decision No 33/99, CRT 17/99, 26 November 1999) and *Proceedings Commissioner v Commissioner of Police* [2000] NZAR 277

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.[60]

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[61]. 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.[62] The NZ Privacy Commissioner has commented:

> "I considered that principle 5 requires more than the existence of a procedure and a training programme, because they do not guarantee the procedure will be followed. To implement a procedure effectively, some steps need to be taken to ensure it is followed. Steps might include retraining on procedures following a particular problem and giving regular training and refresher courses. It might be appropriate to include a disciplinary provision so staff know there will be consequences for failing to follow the procedure. This is particularly important where a procedure has been developed to ensure that customers' needs are met in an area where there is a potential for them to suffer harm."[63]

The NZ Tribunal followed this line of argument in another case involving disclosure by a government welfare agency of sensitive personal details about a client to a volunteer charity worker. The Tribunal found a breach of the security principle in that the issue of unauthorised disclosure was not adequately addressed by the defendant in its training or manual, and that in the context of information about vulnerable clients, the agency's training programme did not sufficiently address these matters so as to enable staff to be clear about their obligations. What was reasonable in the circumstances was a training programme for all front-line staff that included specific training on what information could be disclosed to whom, and what the consequences would be for failure to observe internal protocols on the issue.[64]

---

[60] 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.

[61] [2002] PrivCmrCan PIPEDA 100, 2002 CanLII 42378 (P.C.C.)– a bank's security was found to be adequate despite an unauthorised disclosure by an employee, in contravention of procedures and training

[62] [2001] PrivCmrNZ 17 (Case Note 16005); [1997] NZPrivCmr12 (Case Note 10668)

[63] [1997] NZPrivCmr12 (Case Note 10668)

[64] *W v Director-General of Social Welfare* (unreported, Decision No 11/98, CRT 4/98, 11 June 1998) *and W Director-General of Social Welfare* (1998) 5 HRNZ 580.

Vetting and screening of employees

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.[65] Similarly the Privacy Commissioner of Canada found[66] 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).

Security of client data vs employee privacy

The balancing of security against the privacy rights of employees arises not only in pre-employment checks but also in continuing security measures. Both the New Zealand and the Canadian Commissioners have held employers use of biometrics (fingerscanning in NZ[67] and 'voiceprint' recognition in Canada[68]) to be 'reasonable' even though they involved significant intrusions into employee privacy.

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,

---

[65] [2001] PrivComrNZ 18 (Case Note 21451)

66 [2002] PrivCmrCan PIPEDA 65, 2002 CanLII 42373 (P.C.C.)

[67] [2003] NZPrivCmr5 (Case Note 33623)

[68] [2004] PrivCmrCan PIPEDA 281 *Organization uses biometrics for authentication purposes*, 2004 CanLII 52853 (P.C.C.)

endangering him, was a breach of the security principle in the Hong Kong Ordinance[69]. 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.[70] No other reason is given for the finding, which was not contested[71] . 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.

Can authorised actions result in a security breach?

The security principles in most privacy laws 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 the actions giving rise to a security breach 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 risk of 'loss' is not qualified in any way and on a plain reading would encompass destruction of personal information by

---

[69] http://www.pco.org.hk/english/ordinance/ordfull.html (5-12-06) - Data Protection Principle 4 requires 'practicable steps' to guard against the same risks as the similar principles in Australasian laws.

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

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

the record-keeper or organisation itself. Privacy Commissioners have also taken the view that security must protect against those who have authorised access[72].

However, NZ cases suggest a more restrictive interpretation. In one, the Tribunal found that there was no breach of the requirement for proper security measures in respect of the information, as only authorised staff members and the defendant's legal counsel had access to it. There was no use, modification, or disclosure of the plaintiff's personal information without the defendant's knowledge or authorisation. The Tribunal was satisfied that this allegation had no chance of success because it was "based on a misunderstanding of the scope and meaning of IPP 5"[73]

It may be that both 'misuse' and 'loss' are to be interpreted similarly i.e. as something that the data controller does not intend or do deliberately, as well as consequences that might flow from unauthorised access by or disclosure to third parties.

A recent decision by the NSW Court of Appeal has thrown into doubt the widely accepted assumption that agencies will be vicariously liable for unauthorised disclosures by employees with legitimate access to personal information. It was held that:

> "…'use' or 'disclosure' for a purpose extraneous to any purpose of the Department, it should not be characterised as 'use' or 'disclosure' by or 'conduct' of the Department."[74]

However, the ADT's original finding of a breach of the security principle was not at issue in the subsequent appeals. This was presumably because the responsibility for adequate security remains, and the risk simply becomes one of unauthorised use or disclosure by a third party, rather than of unauthorised use or disclosure by the agency itself. An agency can therefore still be held to have breached the security principle in connection with a 'maverick' action by an employee, if it has not taken 'reasonable steps', including appropriate training (see later).

---

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

[73] *H v Westpac Trust* (unreported, Decision No 28/99, CRT 15/99, DATE)

[74] Director General, Department of Education and Training v MT [2006] NSWCA 270

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[75]).

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'. However, in a case reported only in the Commissioner's Annual Report, a counselling agency was found to have had inadequate security – breaching IPP 5, even though the disclosure of client information concerned was clearly by a casual employee acting other than in the performance of her duties.[76]

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).

---

[75] 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.

[76] *Report of the Privacy Commissioner for the year ended 30 June 2002* (AJHR A.11)

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 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."[77]

Security breaches can also be breaches of disclosure principles

In New Zealand, where the commencement of the Privacy Act was phased, there was a three year period (1993-96) during which the Security principle (IPP 5) was in force but the Disclosure principle was not. A complainant attempted to argue that an unwelcome disclosure of information about their financial affairs was a breach of IPP 5.78 The Tribunal rejected this on the grounds that there was no loss, or unauthorised use or disclosure, of personal information. While a disclosure principle could in theory be used as a substitute for a missing security principle, all current privacy laws contain both, and the point is therefore moot.

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.

---

[77] [2002] PrivCmrCan PIPEDA 41 , 2002 CanLII 42368 (P.C.C.)

[78] *Erwood v Countrywide Banking Corporation Ltd* (unreported, Decision No 2/96, CRT #/#, 6 March 1996)

While belatedly drawing attention to encryption as a tool[79], 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.[80] And in a Report of investigation into a major unauthorised disclosure incident, the Commissioner has recommended the use of encryption for information exchanges between the Office of Police Integrity, and other bodies including Victoria Police.[81]

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[82].
- Putting material about one person in envelopes addressed to another person[83]
- Faxing personal information either to the wrong fax machine[84], or to machines in common areas without taking steps to ensure the intended recipient is on hand to collect the pages[85].

---

[79] 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.

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

[81] 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 …"

[82] HKPrivCmr ar9798-10; [2002] HKPrivCmr 7 (ar0203-6), and [2002] HKPrivCmr 8 (ar0203-7). Also [2003] PrivCmrCan PIPEDA 154 , 2003 CanLII 36261 (P.C.C.) in which the Commissioner held that a bank should institute manual checks to ensure that envelopes containing sensitive personal information are sealed.

[83] [2003] NZ PrivCmr 22 (Case Note 28351); [2002] PrivCmrCan PIPEDA 28 , 2002 CanLII 42313 (P.C.C.)– the bank in question agreed to institute a 'double verification' process in its mailroom

- Printing of sensitive personal information on envelopes[86], or on correspondence visible through envelope windows[87] (Note however that appropriate use of window envelopes has been recommended by the NZ Commissioner as a security precaution.[88])

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 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[89]. A New Zealand case suggests that even wrongly addressed mail need not necessarily imply a failure of security.[90]

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[91]. 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[92]. However, in the latter case the documents in question had ended up scattered on a public footpath, with the potential for public

---

[84] [2001] HKPrivCmr 5; ar0102-5; [2005] PrivCmrA 11.

[85] M v Cth Agency [2003] PrivCmrA 1; [1999] NZPrivCmr 11 (Case Note 13518); [2003] PrivCmrCan PIPEDA 226, 2003 CanLII 48376 (P.C.C.); [2005] PrivCmrCan PIPEDA 317 *Fax from debt collector contained debtor's personal information*, 2005 CanLII 49209 (P.C.C.).

[86] [1998] HKPrivCmr 12 (ar9798-17), [2003] NZ PrivCmr 23 (Case Note 23067)

[87] 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 (5-12-06). An Australian Privacy Act case also dealt with the use of window envelopes but found that a one-off incorrect folding of a letter meant that there was no systemic security breach - [2006] PrivCmrA 20.

[88] [1998] PrivCmrNZ 2 (Case Note 2448) – 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.

[89] [2002] PrivCmrCan PIPEDA 43, 2002 CanLII 42366 (P.C.C.)

[90] [1998] PrivCmrNZ 15 (Case Note 14982)

[91] [1998] PrivCmrNZ 8 (Case Note 6983)

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

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[93];
- 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)[94];
- use of 'real' personal information in training or in publications – such as when illustrating a point with a case study[95], or in providing 'test' databases for training or demonstrations[96], 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[97] on a bank to implement appropriate policies and practices[98].
- failure to provide reasonably confidential facilities for discussion with clients[99].

---

[93] [1998] HKPrivCmr 4 (ar9798-16); [2005] PrivCmrCan PIPEDA 304 *Movie theatre chain strengthens personal information handling practices*, 2005 CanLII 27666 (P.C.C.)

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

[95] [2002] NZPrivCmr 2 (Case Note 26280)

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

[97] 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

[98] HKPCO Newsletter August 2004 - http://www.pco.org.hk/english/publications/newsletter_issue13.html (5-12-06) and [2004] HKPrivCmr 3 (ar0304-7) .

[99] [1995] PrivCmrNZ (Case Note 2594) – no breach in the particular case but the agency agreed to instal a private office.

- the filing of facsimiles on thermal paper which fade over time[100] (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.[101]

Protection against loss of data

Attention to compliance with security principles has focused mainly on the risk of inappropriate use or disclosure. One case has however considered the adequacy of security measures to protect against loss of personal information. The Australian Commissioner reviewed a situation where a medical record had been lost, and found that it appeared that the misplacement of the record was the result of human error and not the result of a systemic procedural problem on the part of the health service provider[102]. Similarly, the NZ Commissioner found no breach of the security principle in Health Rule 5 when a patient record was lost in transfer to another health professional.[103]

Obligations when contracting services

The international privacy instruments place considerable emphasis on the need for data controllers to ensure continued protection when they 'contract out' processing[104].

Some of the Security principles in Australasian laws contain an express reminder of this – requiring agencies to ensure that reasonable steps are taken to prevent security breaches by contractors.[105] However, the more recent private sector NPP 4 omits the express reference to contractors found in IPP 4(b). The more recent laws appear to rely instead

---

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

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

[102] [2006] PrivCmrA 21

[103] [2003] NZPrivCmr 21 (Case Note 26781)

[104] Directive 95/46/EC Articles 16 and 17.2-17.4;

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

on more general obligations on agencies for any actions of contractors[106], or in some cases parallel or separate obligations on contractors themselves, who can also be investigated and held directly liable for breaches[107].

The Australian Privacy Commissioner's report into the theft from the ACT Department, mentioned above, which is of general application, identified 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 privacy compliance just because the actual privacy breach was committed by a contractor. 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[108] . Reference has already been made above to the APRA guidance on outsourcing contracts in financial services needing to cover security matters.

The Australian Privacy Commissioner's 2005 report on her review of the private sector provisions recommended that the government:

> "…consider amending NPP 4 to impose an obligation on an organisation to ensure personal information it discloses to a contractor is protected", and "consider, in the context of the wider review of the Privacy Act, … whether there should be a distinction between data controllers and data operators".[109]

The government's November 2006 response to the Commissioner's report[110] refers these recommendations to the wider Australian Law reform Commission review[111].

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

---

[106] 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).

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

[108] [1998] PrivCmrNZ 6 (Case Note 2663)

[109] Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector provisions of the Privacy Act 1988*, March 2005, p.189 (recommendations 54 and 55).

[110] See http://www.ag.gov.au/www/agd/agd.nsf/Page/Privacy_GovernmentresponsestoPrivacyActreports (4-12-06)

[111] The ALRC Issues Paper 31, October 2006, invites submissions as to whether the security obligation should expressly address contracting (Question 4-17) - see http://www.austlii.edu.au/au/other/alrc/publications/issues/31/

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.[112] 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[113].

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 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[114] 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[115].

Most systems administrators would be aware of the need for regular password changes[116], and for revocation or change to access privileges for staff who leave or have

---

[112] 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)

[113] See [2003] NZPrivCmr 22 (Case Note 28351)

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

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

[116] See [2006] PrivCmrA 8, already cited above.

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.[117]

Another issue that has arisen is the potential risk from 'lag times' or delays between notification of changes and implementation. A case conciliated by the Australian Privacy Commissioner found that a 24 hour processing period allowed inappropriate internet access after a specific request from an account holder to restrict access.[118] Security arrangements need to take account of such potential difficulties.

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[119].

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.

The Commissioner's audit of federal government websites in 2001[120] 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:

---

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

[118] See [2006] PrivCmrA 16

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

[120] Privacy Compliance Audit: Commonwealth Government Web Sites, August 2001 http://www.privacy.gov.au/publications/wsr01.html#_Toc521734767 (5-12-06)

> "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. Further guidance on website security has been issues both by the Privacy Commissioner and the Australian Government Information Management Office.[121]

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.[122] 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).

As noted above, audit reports from other regulators and other jurisdictions often include findings and recommendations expressly about information security, and these are another valuable resource.

A new element – security breach notification

In the last few years, some overseas jurisdictions have introduced security breach notification laws.123 The value of such laws came to international attention in 2005 when the company Choicepoint was required by the Californian law enacted in 2002 to notify 145,000 consumers that their personal information had been sold to a criminal enterprise as a result of a security breach.

---

[121] Office of the Privacy Commissioner Guidelines for Federal and ACT Government Websites- March 2003 - http://www.privacy.gov.au/internet/web/, and AGIMO, The Guide to Minimum Website Standards Security- April 2003 - http://www.agimo.gov.au/practice/mws/security

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

[123] 35 US States had enacted such laws as at January 2007 – see http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm

A similar case in Australia is cited in the ALRC Issues Paper, which also canvasses the issues surrounding such a development[124].

Notification is considered important to allow individuals to take or seek remedial action and/or make informed decisions about whether to continue a relationship. Businesses, and to a lesser extent government agencies, have traditionally been reluctant to publicise security lapses, both because of the potential for reputational damage and, it is sometimes claimed, to avoid giving clues about vulnerabilities that could be used in 'copycat' attacks. Government agency security lapses have sometimes become public knowledge 'after the event' either in their own Annual reports, or through reporting by Auditors-General, Ombudsmen or Privacy Commissioners.

The first reason for not publicising security breaches is precisely one of the main justifications for new security breach notification requirements: on the basis that the risk of reputational damage to the data user will act as a stimulus for improved security measures. The second reason is largely spurious: there is no reason why notification of lapses has to go into the technical detail, and in any case this 'excuse' applies only to third party attacks, and is not valid for breaches that result from carelessness by the data user.

Support for security breach notification requirements is building both in Australia[125] and other jurisdictions[126].

One of the key issues is the threshold criteria that will trigger the requirement for notice. Some of the factors that may be relevant were set out in a 2003 paper from the Californian government.[127] There should now be sufficient experience of the operation of these laws in the USA to provide a sound basis for determining appropriate thresholds.

Conclusion

Reasons for reform - Inter-jurisdictional comparisons

Inter-jurisdictional 'adequacy' is a significant concept in privacy law. All the international instruments aim to facilitate the transfer of information by ensuring that the effect of protective laws in one jurisdiction is not undermined by a lack of protection in others. The 1995 EU Directive codified this objective with provisions requiring member states to limit the transfer of personal data to jurisdictions without 'adequate' laws or

---

[124] Issues Paper 31, at paragraphs 4.204 - 4.207

[125] Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (2005),

[126] See http://www.itworldcanada.com/a/IT-Workplace/33a605d7-cec4-46b0-b617-8fea1451dc6d.html

[127] http://www.ucop.edu/irc/itsec/security_breach_notification.pdf

other safeguards.[128] Similar provisions have been included in all the Australian privacy laws as well as in Hong Kong, although in some cases the provisions have not yet been brought into effect.[129] Potentially, these provisions could have the effect of preventing transfers of personal information between jurisdictions (even within Australia) or at least require either express consent, or extra safeguards in the form of either contracts or other binding agreements.

The overall 'adequacy' of Australia's privacy laws in relation to the European Union Directive remains uncertain – an EU Committee opinion in 2001 found several weaknesses[130], and negotiations are continuing. The government has agreed with the Privacy Commissioner's finding and recommendation that

> "There is no evidence of a broad business push for 'adequacy'. Given the increasing globalisation of information, however, there may be long term benefits for Australia in achieving EU 'adequacy'. Certainly the globalisation of information makes the implementation of frameworks such as APEC important. The Australian Government should continue to work with the European Union on the 'adequacy' of the Privacy Act …"[131]

There has been no suggestion that the security principles in Australian privacy laws are a contributor to any current 'inadequacy'.

Other reasons for reform

While there may be no compelling justification for modifying the security principles to avoid trader barriers, there are many other reasons for pursuing a 'best practice' principle. 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[132], organisations can expect to obtain a clearer view of their obligations, both generally and in a variety of

---

[128] Directive 95/46/EC, Articles 25 & 26

[129] For instance, s.19(2) of the NSW PPIPA only take effect when a Code of Practice has been made by the Commissioner – and despite a requirement that this be done within a year of commencement (1999), no such Code has yet been made. Similarly, the Hong Kong Commissioner has yet to issue a notice to give effect to s.33 of the Personal Data (Privacy) Ordinance.

[130] Article 29 Data Protection Working Party, Opinion 3/2001 – see http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp40en.pdf (4-12-06)

[131] Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector provisions of the Privacy Act 1988*, March 2005 (recommendation 17). Government response, November 2006.

[132] 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.

A best practice model?

The Australian Law Reform Commission's current Review of Privacy[133] provides a timely and appropriate forum for development of a model security principle. One attempt to put forward a 'best practice' standard is the draft Asia Pacific Privacy Charter[134], which proposes:

> "Organisations should protect personal information against unauthorised or accidental access, use, modification, loss or disclosure, or other misuse, by security safeguards commensurate with its sensitivity, and adequate to ensure compliance with these Principles".

This has now arguably been superceded by the more detailed APEC security principle cited above but repeated here:

> "Personal information controllers should protect personal information that they hold with appropriate safeguards against risks, such as loss or unauthorized access to personal information, or unauthorized destruction, use, modification or disclosure of information or other misuses. Such safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment." (APEC Privacy Framework 2005, Principle VII)

This formulation of the principle appears to offer clear guidance and to incorporate concepts of risk management and proportionality which should benefit both data subjects in terms of added protection, and data controllers in terms of compliance costs.

---

[133] http://www.alrc.gov.au/inquiries/current/privacy/index.htm

[134] The Asia Pacific Charter will be further developed over the coming year, partly based on the work of this Interpreting Privacy Principles project, and the draft security principle in the Charter will take account of the experience summarised in this paper.