Working Paper No 2

Interpreting Retention and Disposal Principles

v.1 September 2006

Nigel Waters, Principal Researcher, Interpreting Privacy Principles Project, Cyberspace Law and Policy Centre, University of New South Wales, http://www.cyberlawcentre.org/ipp/

This paper is a revised and updated version of an article entitled *IPPs examined: The retention principle*, by Nigel Waters and Graham Greenleaf, published in Privacy Law & Policy Reporter, Volume 11 No 4 in October 2004

DRAFT

CONTENTS

Introduction

Most privacy laws contain a principle dealing with the retention and disposal of personal information. In some laws it stands alone as a separate principle, while in others it is found within the security principle.

Most organisations subject to privacy law retention and disposal principles will have to reconcile their specific obligations in relation to personal information with general retention and disposal obligations under other laws, and this interaction is a major focus of the following discussion.

Privacy Legislation

The principles in Australasian privacy laws that deal with retention and disposal are all very similar in effect though there are significant differences in the way they are expressed – some approaching from the retention end and some from the disposal perspective.

The first set of legislated principles – the Information Privacy Principles or IPPs in the federal *Privacy Act 1988* – did not contain any provisions concerning retention or disposal. Despite the absence of an express retention and disposal principle the Australian Federal Commissioner made several references to an implicit requirement in reports of investigations and audits in the first ten years of operation of the Act[1].

The New Zealand Act, a few years later, introduced a separate retention principle:

> "Principle 9: Agency not to keep personal information longer than is necessary
>
> An agency that holds personal information shall not keep that information for longer than is required for the purpose for which the information may lawfully be used."[2]

The NSW law includes provisions relating to retention and disposal as the first part of a retention and security principle:

> "A public sector agency that holds personal information must ensure:
>
> (a) that the information is kept no longer than is *necessary* for the purpose for which the information may lawfully be used (emphasis added), and

---

[1] Including Annual Report 1994-95, pp67-68 unfair retention of irrelevant psychological assessment); p147 (failure to follow Archives Act disposal schedule); p183 (failure to keep register of requests); AR 1998-99, p67 (employment service providers retaining jobseeker records in breach of rules)

[2] Privacy Act 1993 (NZ) s.6 – Principle 9

> (b) that the information is disposed of securely and in accordance with any requirements for the retention and disposal of personal information, …"[3]

In the private sector NPPs, introduced into the federal Privacy Act in 2000, the Data Security principle includes:

> " 4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose for which the information may be used or disclosed under NPP 2."[4]

This formulation is also used in the Victorian[5] and Northern Territory[6] laws.

The Data Protection Principles (DPPs) in the Hong Kong Ordinance include a further variation of the negative formulation:

> "Personal data shall not be kept longer than is necessary for the fulfilment of the purpose (including any directly related purpose) for which the data are or are to be used"[7]

The HK Ordinance also contains a positive formulation in s26(1):

> 'A data user shall erase personal data held by the data user where the data are no longer required for the purpose (including any directly related purpose) for which the data were used unless-
>
> (a) any such erasure is prohibited under any law; or
>
> (b) it is in the public interest (including historical interest) for the data not to be erased.'

A novel provision in s26(2)(b) provides that the 'data user shall not be liable in an action for damages at the suit of the second-mentioned data user in respect of any such erasure'. This protects data users against claims that by erasing a person's persons data (possibly to the prejudice of the person) they have therefore breached the security principle – provided that all purposes for which the data was used have expired.

The Canadian federal law applying to the private sector – the *Personal Information Protection and Electronic Documents Act* also has a negative general obligation:

---

[3] Privacy and Personal Information Protection Act 1998 (NSW), s.12. – known as Information Protection Principle (IPP) 5. Inexplicably, investigative agencies are expressly exempted by s.24(7) from the requirement of s.12(a).

[4] Privacy Act 1988 (Cth) Schedule 3, Clause 4 – known as National Privacy Principle (NPP) 4.

[5] Information Privacy Act 2000 (Vic), Information Privacy Principle (IPP) 4.2

[6] Information Act (NT), Information Privacy Principle (IPP) 4.2

[7] Personal Data (Privacy) Ordinance 1995, Schedule 1, Data Protection Principle (DPP) 2(2)

> "Personal information shall be retained only as long as necessary for the fulfilment of (the purposes for which it was collected)" (Principle 4.5),

but goes further in prescribing detailed positive requirements:

> "Organizations should develop guidelines and implement procedures with respect to the retention of personal information. These guidelines should include minimum and maximum retention periods. Personal information that has been used to make a decision about an individual shall be retained long enough to allow the individual access to the information after the decision has been made. An organization may be subject to legislative requirements with respect to retention periods". (Principle 4.5.2), and
>
> "Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous. Organizations shall develop guidelines and implement procedures to govern the destruction of personal information." (Principle 4.5.3)

Canadian commentators debate the merits of including such non-mandatory ('should') statements in the legislation[8].

The Canadian federal public sector *Privacy Act 1985* contains both retention and disposal principles (in s.6) but both are only made operational by specific regulations or ministerial guidelines or directives. The objective of the retention regulations[9], which require retention for at least two years after the last administrative use, is to ensure that personal information is available to the individual to whom it pertains if requested.

In some sectoral legislation such as the credit reporting provisions of the *Privacy Act 1988 (Cth)* Part IIIA there are detailed deletion principles with specified time limits for retention of categories of information[10]. The statutory Tax File Number Guidelines issued by the Australian Federal Commissioner under the same Act contain a permissive rule – "Tax file number recipients may dispose of tax file number information when it is no longer required by law nor administratively necessary to be retained."[11]

In terms of subordinate legislation, the Hong Kong Privacy Commissioner has issued Codes of Practice in areas such as Consumer Credit Data[12] and Human Resources

---

[8] ch S Perrin, H Black, D Flaherty and M Rankin *The Personal Information Protection and Electronic Documents Act - An Annotated Guide* Irwin Law, Toronto, 2001, [4.5.3]

[9] Privacy Regulations [SOR/83-508]

[10] Eg: Privacy Act 1988 (Cth) s.18F.

[11] Tax File Number Guidelines 1992, Guideline 6.2.

[12] See http://www.pco.org.hk/english/publications/files/CCDCode_eng.pdf

Management[13] which in some cases specify periods of retention for specific categories of data. The first Codes issued by the New Zealand Privacy Commissioner[14], do little more than re-state the retention principles in their respective Acts, although for the NZ Credit Information Privacy Code 2004 prescribes specific retention periods as in the Australian Credit Reporting regime[15]. Similarly, some of the Codes approved by the Australian Privacy Commissioner[16] merely re-stated the statutory retention principle. But two of the Codes contain supplementary rules on disposal for particular 'industries'.

The Biometrics Institute Privacy Code, approved in 2006, and which applies to members in both Australia (where it is binding) and New Zealand (where it is only advisory), contains a number of additional principles about retention and disposal[17]. These are:

> "Wherever practicable, a Code Subscriber shall ensure that biometric information is encrypted immediately after collection, that the original biometric information is destroyed after encryption and that biometric information is stored only in encrypted form) (11.1)
>
> Unless required by law, biometric information shall remain in storage only as long as is necessary for the proper functioning of the biometric system for which it was collected. (11.3)
>
> After personal information is no longer needed for any purpose for which it may be used or disclosed under Biometrics Institute Privacy Principle 2, it shall be destroyed or otherwise disposed of in a secure manner as outlined in Biometrics Institute Privacy Principle 4.2 (11.4)"

The 2003 Market and Social Research Privacy Code[18] customises the first security principle to read

> "A research organisation may retain identified information only whiel the details of the identity of the individual whom the information is about continue to be necessary for research purposes" (4.1)

---

[13] See http://www.pco.org.hk/english/ordinance/files/hrdesp.pdf

[14] Telecommunications Information Privacy Code 2003 ; Health Information Privacy Code 1994 (as amended) – see http://www.privacy.org.nz/comply/codes.html

[15] Credit Information Privacy Code 2004, Rule 9 and Schedule 1. see http://www.privacy.org.nz/filestore/docfiles/49179009.doc

[16] See http://www.privacy.gov.au/business/codes/index.html#1

[17] See http://www.biometricsinstitute.org/

[18] This Code was under review in September 2006 see http://www.amro.com.au/index.cfm?p=2403

No 'reasonable steps' qualification in some Acts

Unlike many of the other privacy principles, the retention and disposal obligations are not qualified in some Acts (NSW, NZ, HK and Canada) so as to require only 'reasonable' or 'reasonably practicable' steps – the obligation is expressed in absolute terms. The 'reasonable steps' qualification in principle 4.2 of the Australian private sector, Victorian and Northern Territory regimes is the exception to this.

It will be interesting to see if the regulators and the Courts import a 'reasonable steps' consideration into their enforcement of this principle where it is not expressly provided. Where organisations have very large data collections, particularly on paper or in legacy databases, it may be extremely costly to set up regimes to identify when each individual data item passes its 'no further use' date. In these cases, if organisations have procedures for periodically reviewing and culling data according to some generic rules, it would be surprising if the fact that specific data items were not immediately culled resulted in breaches of this principle being found.

Sources of interpretation

Even with an apparently unambiguous obligation, organisations subject to a privacy law are understandably uneasy about what compliance means in practice. They will look ultimately to decisions of tribunals and courts for the standards required in different circumstances.

While there are a few Court and Tribunal decisions available, organisations have also had to rely on the opinions of the regulators as expressed in guidance material, in the reports of conciliated cases published by some Privacy Commissioners, and in the reports of special investigations and audits conducted by those Commissioners who have those functions[19]. These are considered in the rest of this paper.

Some guidance may also be found in textbooks on regional privacy laws[20].

De-identification

It is important to recognise that there are two possible options once a deletion principle takes effect on personal information. The first is deletion or destruction, but there is also a second option – de-identification.

---

19 The Australian 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.

20 These include M Paterson [2005] Freedom of Information and Privacy In Australia, LexisNexis Butterworths; M Berthold & Wacks [2003] *Hong Kong Data Privacy Law*, 2nd Edition Thomson Sweet & Maxwell; and Perrin, Black, Flaherty and Rankin [2001] *The Personal Information Protection and Electronic Documents Act - An Annotated Guide* Irwin Law, Toronto,

The identical disposal principles in the Australian private sector, Victorian and NT laws explicitly includes anonymisation ('permanently de-identify') as an alternative to destruction of personal data, whereas the principles in other laws do not. However, the other laws say that organisations shall not 'keep' 'personal information' (not 'records') longer than is necessary, and it can be argued that personal information is not 'kept' if it is permanently de-identified, because then the information that remains will not satisfy the definition of 'personal information' (it will not be capable of being used to identify the person). If this is so, then all retention principles allow both destruction of records and de-identification of personal data as methods of compliance.

The Australian Privacy Commissioner's NPP guidelines take a similar approach, stating that de-identification 'means that an organisation is not able to match the de-identified information with other records to re-establish the identity of people'[21]

The Australian Privacy Commissioner has dealt specifically with the interaction of destruction and de-identification in Guideline 3 of the Medicare and Pharmaceutical Benefits Programs Privacy Guidelines 1997.[22] However, in a recent review of these Guidelines the Commissioner has proposed relaxing some of the destruction rules – allowing Medicare Australian to keep claims information indefinitely, subject to safeguards, which include separating identifying particulars after 5 years and strictly controlling subsequent linkage for re-identification.[23]

There is a whole area of debate about what is actually meant by de-identification, as it is often at least theoretically possible to re-identify at least some individuals from other details, particularly by someone with special knowledge. But this issue will not be pursued further in this paper.

Relationship to other retention requirements

There should always be a retention period, and associated disposal timetable, directly associated with the original purpose of collection of any personal information. In some cases this will derive solely from the business needs of the organisation that holds the information, and in others from associated legal requirements, which may include statutory obligations, but also prudential and other defensive reasons, such as to protect against future litigation.

All privacy laws accept the proposition that the justification for retention may be unrelated to the original specific purpose of the organisation holding personal information. This is usually expressed in two ways. Firstly by linking the disposal requirement to any purpose permitted by the use principle, which invariably includes

---

[21] Privacy Commissioner 'Guidelines to the National Privacy Principles', 2001, p.46.

[22] See http://www.privacy.gov.au/publications/mapbp.pdf

[23] See http://www.privacy.gov.au/news/06_13.html

both secondary related purposes and unrelated 'public interest' uses. Secondly by a general 'or otherwise authorised or required by or under law' exception.

The one exception to the first norm is the Canadian private sector law, which allows retention only for a purpose of collection (emphasis added), and not for other purposes even where they are permitted under the use principle. This is potentially a very important distinction, as it means that personal information will only be available for unrelated third party purposes during the period for which it can be justified by reference to the original purpose, unless there is a specific legal retention requirement for those other purposes. In contrast, the other laws allow personal information to be retained solely for the other purposes, provided they can be justified under the use principle.

A good topical example would be the retention of customer information, such as call charge records by a telecommunications provider, beyond the period for which there is a commercial justification, on the basis of a perceived need to assist law enforcement agencies – a secondary use and disclosure which is permitted under most privacy laws. This specific issue of retention of telecommunications traffic records has been hotly debated in the context of international conventions on Telecommunications Privacy and Cybercrime. [24]

In Australia, the Internet Industry Association has proposed a Cybercrime Code of Practice which would set standards for retention of traffic data by Internet Service Providers. While controversial, the Code, if it could be agreed, could provide useful guidance on how to balance requirements in privacy and other laws.[25]

Other legal requirements will normally prevail…

Where there is a specific *requirement* in another law for retention of personal information, that will normally 'trump' the disposal principle in a general privacy law.

There are many such statutory retention requirements. Most public sector agencies are subject to Public Records or Archives Acts which generally require retention of many categories of records, and also impose a disciplined and systematic approach to disposal, usually with express recognition of privacy interests in relation to personal information.

Many private sector businesses are subject to record-keeping and retention requirements in financial and corporate regulations, while similar obligations in relation to the environmental regulation, health and safety and industrial relations can apply across both public and private sectors.

One of the most commonly referenced retention requirements is the period for which the Australian Taxation Office requires taxpayers to keep evidence to substantiate taxation

---

[24] See the European Union Directive 2002/58 on Privacy and Electronic Communications, Article 6, at http://europa.eu.int/comm/internal_market/privacy/law_en.htm and the Council of Europe Cybercrime Convention at http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

[25] See http://www.iia.net.au/cybercrimecode.html - particularly clause 7.

claims. Definitive advice on this requirement is elusive, but one page of the ATO's website includes the statement:

"The most important reason for keeping good records is that it's a legal requirement for you to do so. By law, the Tax Office requires you to keep business records:

for five years after they are prepared, obtained or the transactions completed (whichever occurs later), and ...."Other pages refer to keeping sales and purchase invoices and records of payments to employees. While it is not clear that the taxation requirement necessitates retention of all *personal* information held by a business (much of which will not be directly relevant to taxation liability), there is an understandable tendency to 'play it safe' and use 'five years' as a general rule of thumb for all records.

The ATO website warns that:

> "Other regulatory bodies may have different record keeping requirements from the Tax Office, particularly around how long you have to keep records."

A good example is that under the Financial Transaction Reports Act 1988 all cash dealers (including most banks and other financial institutions) are required to retain account and signatory information for seven years after the day on which an account is closed.[26] The proposed replacement legislation maintains this seven year period and extends it to other records.[27]

Another factor is the increasingly 'front of mind' prospect of litigation. While there have been many well-publicised cases of embarrassment, or worse, from records kept unintentionally, there have also been cases where failure to keep adequate records has hindered a defence. In Victoria, legislation now makes it a criminal offence to destroy documents that are 'reasonably likely to be used in evidence in legal proceedings that may have begun or may begin in future' (emphasis added).[28]

It would be easy for managers to take the view that a combination of specific requirements; general 'due diligence' obligations and overall prudence in anticipation of future complaints or litigation combine to justify a general policy of keeping most records indefinitely. Certainly this would seem to be the advice that many businesses are receiving in relation to E-mails, telephone records and general customer transaction records.

---

[26] What are the FTR Act's document retention requirements? in Module 13 of the AUSTRAC eLearning application study guide at http://www.austrac.gov.au/aml_elearning/

[27] Revised Draft Exposure Anti-Money Laundering and Counter-Terrorism Financing Bill 2006, Part 10. See http://www.ag.gov.au/agd/WWW/agdhome.nsf/Page/RWP8B2E91AF7CF4CFCACA2570C900112F4C

[28] *Evidence (Document Unavailability) Act 2006* (Vic)

… but only if specific

But it would be unwise for agencies or organisations to assume that a general record retention requirement, whether statutory, common law or otherwise, will have the effect of trumping disposal obligations in privacy laws if the former requirement does not *expressly* address the issue of *personal* information.

It is quite possible to reconcile in theory a general record retention provision with the disposal of personal information principle by selective editing. However the difficulty or cost of doing so would normally make such a step unreasonable, and a judgement will be needed as to which requirement should prevail.

In GR v Dept of Housing [2003] NSWADT 268, the NSW ADT considered the interaction of the State Records Act 1998 (SRA) and the disposal principle in PPIPA (IPP 5, s.12). Section 12(1) of the SRA provides that "Each public office must make and keep full and accurate records of the activities of the office". s21(7) of the SRA provides that an Act enacted after the commencement of the section "is not to be interpreted as prevailing over or otherwise altering the effect or operation of this section except insofar as that Act provides expressly for that Act to have effect despite this section".

The NSW Privacy Commissioner submitted to the ADT that the State Records Act and the Privacy Act should be read together in harmony, and that there are several provisions in the PPIPA that show an awareness of possible conflict with the SRA and suggest that there was an intention to reduce or minimise such conflict.

Two of the provisions referred to by the Commissioner support the view that the PPIPA Act authorises alteration, and by implication deletion, of records where necessary. Section 20(4) expressly states that the correction principle (IPP8, s.15) applies despite the SRA. Section 25(b) of PPIPA, which provides an exemption from many of the IPPs where non-compliance is otherwise permitted (or is necessarily implied or reasonably contemplated) under an Act or any other law (including, *expressly* the State Records Act 1998), does not apply to the disposal principle IPP5, which must therefore be presumed to prevail.

The respondent in GR submitted that the Tribunal should read down section 15 of the Privacy Act (when it is read with the State Records Act) so as to hold that the only "amendments" that can properly be made pursuant to section 15(1) are notations made pursuant to section 15(2) of the Privacy Act (ie: that deletion was not an option). The Tribunal was not prepared to give section 15 that operation but did not consider it needed to resolve the issue of the operation of the two statutes in the present case. This was because the photographs at issue were in the Tribunal's view clearly relevant to the respondent's functions in maintaining a file on the applicant's tenancy history.

Justification for retention

In a 1996 case, [1996] NZPrivCmr 3 (Case Note 5532), the NZ Privacy Commissioner formed the view that an employer was entitled to keep information about a proposed dismissal (subsequently withdrawn after resolution of a grievance involving the

employee's resignation) against the possibility of further legal action. The employer's standard practice was to retain personnel files for a period of five years after an employee had left.

Two years later, in another case, [1998] NZPrivCmr10 (Case Note 13066), the NZ Commissioner again supported an employer's right to retain adverse personnel information, notwithstanding an agreement to remove it from the employee's active personnel file. The Commissioner agreed that the employer had a 'lawful purpose' for retaining in another place the information which had been removed from the file, since it might have been relevant to the employee's continued suitability. The agreement to remove the information from the personal file had not specified what would happen to it and there was no record of an agreement to destroy the information or refrain from using it in the future.

In a major and lengthy decision in 2005 on three appeals by Police Forces against enforcement notices by the UK Information Commissioner, the UK Information Tribunal canvassed many issues relating to the retention of criminal conviction information on the Police National Computer.[29] Leaving aside the specifics of these cases, the decision provides helpful guidance on the sorts of considerations that apply to the application of retention and disposal principles (in these cases the Fifth Data Protection Principle in the 1998 Data Protection Act) and their relationship to other data protection principles. In particular, it highlights a 'compromise' position of accepting the justification for retention for one purpose (in this case operational policing) whilst limiting access to it to prevent its use for other purposes (in these cases employment vetting).

These appeal case decisions also re-inforced the importance, at least for major databases, of having a clearly articulated and justified policy on retention and disposal – see next section of this paper.

Ad hoc disposal or policies required?

The only decision to date on retention and disposal under the Australian *Privacy Act 1988* to date has sent an important message about the need for been the 2004 determination by the Privacy Commissioner on the operation of a tenancy database service, TICA Default Tenancy Control Pty Ltd or TICA. In Complaint Determination No. 3 of 2004, the Australian Federal Privacy Commissioner found that that TICA had breached NPP 4.2 by failing to take reasonable steps to destroy or de-identify personal information. TICA was removing out-of-date personal information to a 'dead tenants' database'. The Commissioner found this step to be "not reasonable in the circumstances for the following reasons:

- TICA does not appear to have in place reasonable measures to decide when personal information is out-of-date;

[29] South Yorkshire and North Wales Police v The Information Commissioner [2005] UKIT DA_05_0010 (12 October 2005)

- TICA does not appear to take any steps to destroy (as opposed to move) personal information that is out-of-date; and
- Although the 'dead tenant database' is only available to TICA, and is not disclosed outside of the organisation, it does not de-identify the information it contains."

While the Commissioner took the view that his Determination could not specify appropriate retention periods, he made accompanying 'recommendations' which included a maximum of four and three years respectively for tenancy history and enquiries information; and deletion of information moved to the 'dead tenant database' (that is the database which stores deleted listings) not less than once a month (He believed it is acceptable to hold information temporarily in the 'dead tenant database' to ensure that information which is 'accidentally' deleted can be retrieved).

This TICA determination also illustrates the close relationship between the retention and disposal and data quality principles. The Commissioner's findings, in the same Determination, about quality (fitness for purpose) were a pre-requisite for the finding about retention and disposal.

The NSW law has so far not proved as powerful in requiring positive retention and disposal policies. In FH v NSW Department of Corrective Services [2003] NSWADT 72, the applicant – a former prisoner, argued that inmate records should not be retained at all once they leave the prison system and especially where their conviction had been quashed (as it had in his case). However, the Tribunal accepted the respondent's justifications for retaining ex-inmate records, even though they were not laid down in any considered policy. They included the possibility of litigation, the use of records by police as an intelligence resource and the need for information regarding custody where the former inmate re-enters the correctional system. The Tribunal found that the period of retention to date was not unreasonable having regard to those reasons. The respondent acknowledged that 'at some point' it would require a policy on long-term record retention and disposal, but the Tribunal did not take the opportunity to mandate this.

In contrast, the Canadian private sector law makes it much easier to hold an organization to account as it requires not just an appropriate retention decision in individual circumstances, but also a specific retention policy. Three cases illustrate its application, and support the conclusion reached by the Australian Commissioner in the TICA case.

In [2002] PrivCmrCan PIPEDA Case Summary #52, the Canadian Commissioner determined that the respondent company had not previously had retention and deletion policies in place, and had therefore failed to meet its obligations under Principles 4.5.2 and 4.5.3.

In [2004] PrivCmrCan PIPEDA Case Summary #255, the Assistant Commissioner found that while an airport authority had policies regarding the destruction of information, there were none dictating the length of time that information can be kept. The authority kept the information it collected for restricted area passes for all employees in the event that some who leave may return to the airport to work. Although the authority thought it was saving steps by keeping this information, the authority also acknowledged that a new application form would have to be filled out and a new photograph possibly taken should

a former employee return to the airport to work. Therefore, the Assistant Commissioner did not think that such a practice fulfilled any purpose, and she found the authority in contravention of Principle 4.5.

In [2002] PrivCmrCan PIPEDA Case Summary #73 the Canadian Commissioner determined that a telecommunications company's practices with respect to the retention of personal information were inconsistent. The company lacked a policy and procedures, and in default, granted its managers considerable discretion with respect to which documents should be held on file. The Commissioner found the complainant's expectation that there be a degree of consistency regarding retention practices perfectly reasonable. As a result of the inconsistency, the Commissioner made a finding of a breach of the data quality principle.

Compliance with retention and disposal policies

Assuming organisations have a retention and disposal policy in place, whether statutorily prescribed or developed in-house to meet a general obligation, they will also be held to account for ensuring that the policy is followed.

The Australian Federal Privacy Commissioner has periodically reported on the results of audits which revealed failures to follow clearly set-out policies.[30]

Premature disposal

The retention/disposal principle do not excuse premature disposal, which may breach the security principle if a prejudices a person's interests.[31]

The NZ Commissioner, in [1995] NZPrivCmr15 (CN 3984), expressed serious concern about the destruction of information that was the subject of an access request under rule 6 of the Health Information Privacy Code 1994. A hospital, having edited a nine-hour video to a three to five minute segment to respond to an access request, erased the remainder of the tapes. The hospital said it was 'standard practice' to reuse tapes after editing the relevant information, but the Commissioner proceeded to investigate a possible breach of the security rule in the Code, on the grounds that the destruction breached the requirement for reasonable security against loss. The case was settled, with a compensation payment, before any finding, but illustrates how the retention and security principles can interact to require continued storage.

However, two other cases under the same law show that if an organization can demonstrate that it has a well argued case for a particular period they will satisfy the

---

[30] Annual Report 1992-93 p12 (tax file number information unnecessarily retained after use); AR 1993-94, p67 (unnecessary retention of tax file numbers on AUSTUDY forms); AR 1995-96, p195 (failure to follow statutory destruction requirements for Medicare and Pharmaceutical Benefits claims information)

[31] Only the HK ordinance gives any protection against this potential breach of security, through s26(2).

principle, notwithstanding that the disposal proves inconvenient for particular individuals.

In [2003] PrivCmrCan PIPEDA Case Summary #157, the complainant believed that it was wrong of a credit reporting agency to have destroyed past records reflecting a more positive period in his credit history. However the Canadian Privacy Commissioner accepted the premise that that a credit reporting agency's essential purpose was to provide credit grantors with current information on the financial performance of credit applicants. He was satisfied that the six-year retention period adopted by the agency in observance of provincial legislation was adequate for the fulfilment of that purpose. He was also satisfied that the company did have in place appropriate guidelines and procedures regarding the retention of personal information. He found therefore that the agency was in compliance with the relevant Principles.

In [2003] PrivCmrCan PIPEDA Case Summary #252 however, the Assistant Canadian Privacy Commissioner found that a bank was entitled to dispose of acknowledgement letters since the information contained in them existed elsewhere in the bank's records – the principle applies to the information not the specific document. The principle in the Canadian private sector law makes it easier for an individual to insist on retention, by expressly requiring specification of minimum as well as maximum retention periods. But as in the cases under the NZ law, it seems regulators will leave generally leave the length of the retention period up to the organization concerned to decide.

Guidance on retention periods

Guidance on appropriate periods will gradually emerge from Court and tribunal rulings and more likely, from rulings and case studies from regulators.

In an incidental finding in an access case, [2002] PrivCmrCan PIPEDA Case Summary #32, the Canadian Commissioner noted that the respondent company routinely destroyed supervisors' files, in accordance with the company's retention-and-disposal policy, two years after termination of employment.

The Australian Federal Privacy Commissioner, in his guidance on the operation of the Credit reporting provisions of the Privacy Act 1988 (Cth), has specified 12 months as a reasonable minimum period for which rejected credit application be maintained – to tie in with the period beyond which the Commissioner can decline to investigate a complaint.[32]

The Australian Commissioner also considered retention periods in a case involving a retail company which had recorded the fact that it had accused an individual of theft, with which they had subsequently been charged. Having found that the recording of this

[32] See Credit Reporting Advice Summaries 11.8, Retention of Credit applications, at http://www.privacy.gov.au/publications/casw6.pdf

information was lawful, the Commissioner also accepted the retailers policy of deleting such information, with some unspecified exceptions, after five years[33].

In a 1999 HK case, the AAB upheld a determination by the HK Privacy Commissioner that had found that a telecommunications company's policy of retaining customer records for 18 months after account termination, to enable the efficient re-connection of service if required, was appropriate.[34]

Deletion of specific information under correction principles

Whatever the general policy of an organisation on retention and disposal, there may always be exceptional need to delete specific personal information in particular cases, in advance of any general timetable. This may arise from the operation of the correction principles in privacy or, for the public sector, in Freedom of Information laws. The operation of these principles will be considered in detail in a separate paper, but it should be noted that some (not all) such principles include a right to delete information (alternatively expressed as 'striking out', 'obliterating', or 'removing' in some specified circumstances.[35] This right is typically spelt out in some detail in FOI laws as, in the public sector context, it is usually necessary to provide a clear basis for overriding a presumption of retention in Public Record or Archives laws.[36]

New technology issues - Internet archives

The Internet poses some new problems in relation to personal information which it was permissible to place on an Internet website but the uses of which have now finished. Even though an organization may remove the information from its website, a copy of it may still be found in the archives of Internet search engines (and general archives such as the WayBack Machine / Internet Archive[37]. If the personal information could properly be disclosed to the Internet search engine / archive, then the organisation disclosing it will not normally be responsible for the archive deleting it. However, where there has been any wrongful disclosure of information, or breach of security, the organisation may have to seek deletion from the search engine or the archive operator[38].Publication, whether on the Internet or by other means, also brings into play the provisions of some privacy laws

---

[33] See [2006] PrivCmrA 8

[34] See http://www.worldlii.org/hk/cases/HKPrivCmrAAB/1999/3.html

[35] The decision in Doelle and Legal Aid Office (Qld) [1993] QICmr 5 (24 November 1993); (1993) 1 QAR 207 contains a useful analysis of the extent to which correction rights in Australian FOI laws encompass compete destruction of information.

[36] Other examples of cases considering this balance include Borthwick and Town of Victoria Park, Re [2002] WAICmr 29 (13 August 2002); Phillip Patrick Murrin and Police Force of Western Australia, Re [2004] WAICmr 1 (12 January 2004)

[37] See http://www.archive.org/

[38] See Complainant v Statutory Entity [2004] VicPCmr 3, summarised at (2004) 11 PLPR 76

relating to publicly available information. Some laws exempt such information altogether, while others modify the operation of the Principles.

Conclusion

Privacy case law in several jurisdictions is gradually throwing some light on what matters organisations are expected to consider under privacy laws in making decisions on retention and disposal of personal information. 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 summarised, organisations can expect to obtain a clearer view of their obligations, both generally and in a variety of specific circumstances.