BIOGRAPHICAL NOTE

Livia Iacovino is a Lecturer in the School of Information Management and Systems, Monash University. She is also a Principal Researcher in the School's Records Continuum Research Group and the Monash Enterprise Information Research Group. Previous appointments include the National Archives of Australia, the Public Record Office Victoria, and records consultancy work. She has taught and assisted in developing the Monash recordkeeping courses, in particular the legal and ethics curricula. Her publications on the legal-recordkeeping nexus include Things in Action: Teaching Law to Recordkeeping Professionals. Livia was awarded the Australian Society of Archivists Inc. Mander Jones Award, 1999 for 'Recordkeeping and the Law', theme issue, November 1998, Archives and Manuscripts. She is currently in receipt of a Ph.D scholarship.

Identity, Trust and Privacy: Some Recordkeeping Implications in the Context of Recent Australian Privacy Legislative Initiatives *

LIVIA IACOVINO

INTRODUCTION

Business[1] transactions need to be trustworthy if they are to provide evidence of rights and obligations, and serve as personal, corporate and collective memory. The identity of the participants in the business process needs to be captured and retained as part of the metadata of the record, and is essential to the record's authenticity. Information privacy principles are generally concerned that the identity of the participants and the record or data-subject (which constitute identifiable personal data as defined in most privacy legislation) is retained only for its immediate use, or for limited other uses. While the widespread abuse of privacy, in particular in the online environment, requires strong legislative protection, it should not eliminate future access for third parties to reliable evidence.[2]

Recent Australian privacy legislative initiatives, in particular in the Federal and Victorian jurisdictions, extend the ambit of privacy legislation in some cases to the private sector, by adopting an all-inclusive definition of 'organisation', but with complex exemptions and by introducing different types of personal information, in particular health and other 'sensitive' information. While the new legislation extends access and amendment rights to personal information, and requires the consensual collection of personal information that depends on quality recordkeeping, a detailed examination of some key provisions reveal important implications for record trustworthiness.

TRUSTWORTHY RECORDS

Trust in its social context is concerned with faith in someone or something, and identity is a condition or fact that a person or thing is itself and not something else. Identity can be viewed as personal, corporate, professional, and group identity (collective identity), defined by law, conventions and societal mores.[3]

In relation to records, Heather MacNeil has focused on two qualities of a trustworthy record.

When a record is said to be trustworthy, it means that it is both an accurate statement of facts and a genuine manifestation of those facts. Record trustworthiness thus has two qualitative dimensions: *reliability* and *authenticity*. Reliability means that the record is capable of standing for the facts to which it attests, while authenticity means that the record is what it claims to be.[4]

Reliability is never an absolute, but rather there are degrees of reliability due to the dependence of accurate content on individual 'truthfulness'. The degree of reliability of the contents of a record depends on how much is captured of the identity of the persons involved in the record's creation, their credibility, their authority, (their competencies), and the consent of parties to the transaction, while authenticity depends on ensuring that the record's reliability has not been compromised by tampering during or after transmission. Authenticity requires that the elements of record identity (who wrote it, who received it and when) and integrity (completeness) have not been altered.[5]

Although a record may be authentic at the time of its creation (the identity and integrity elements are all present and relied upon by the business), its authenticity over time depends on ensuring that the essential attributes of identity and integrity have not been lost or corrupted.[6] For electronic business purposes authentication is limited to preventing repudiation and fraud by the buyer or seller, and includes the use of electronic signatures for identifying the author of an offer and acceptance of a product.

WHAT IS PRIVACY?

HOW IS TRUST AND IDENTITY RELEVANT TO PRIVACY?

Privacy is recognised internationally as a human right. The International Covenant on Civil and Political Rights 1966[7] provides a definition which emphasises personal integrity and dignity:

1. No one shall be subjected to arbitrary and unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everyone has the right to protection of the law against such interference or attacks.

Personal information as defined in *Privacy Act* 1988, (Cth) Part II, Section 6 means 'information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion'. This definition is used in all the Australian Privacy Acts.

Rights in relation to information privacy (e.g. right of access, rather than a right to privacy) are principally about controlling information others hold about one and include:

- access to and correction/amendment of personal data, and
- how, why and by whom it is collected, handled, stored, transferred and re-used, whether it is held in a database, a recordkeeping system or a network server.

Personal information is at risk when it is transmitted either in the form of:

- Identification of parties to the transaction (record identity),
- Record/data subject identification (record identity and integrity), and
- Third parties holding information about the above: e.g. held by ISP's, authentication certificate providers etc., (record identity).

The identity of parties to the transaction or information which makes it possible to infer the identity and data subject would constitute personal data, and be subject to privacy legislation depending on the jurisdiction and ambit of the legislation.

Identity and trust depend on access to knowledge about the person with whom one is dealing, and trust increases if the moral views, the professional standing, the reputation of the organisation which a person represents, and the authority of the action are known to the transacting parties.

Key recordkeeping questions that need to be resolved in balancing identity, trust and privacy are:

- If individuals need to know with whom they are dealing to maintain trust, how should that information be restricted from third parties?
- If the identification of the parties to a transaction is an essential part of assessing the reliability of its content, how does this impinge on privacy?
- Is there a time limit to when identifying data should be protected?

RELIABLE AND AUTHENTIC RECORDS: CONFLICTS WITH PRIVACY PRINCIPLES

Recordkeeping concerns regarding privacy centre on records that may need to be retained to ensure that the rights and obligations of those affected by the business transaction are protected, and that the related identity metadata are also retained. Long term corporate and collective memory also depends on reliable and authentic evidence. In this context the recent privacy initiatives do not altogether accommodate recordkeeping principles of reliability and authenticity over time.

The privacy principles enshrined in the new Acts do not take account of the record's functional context and the effect of the lapse of time on de-sensitising personal information. Instead they encourage the de-identification or the destruction of records containing personal information no longer required for their immediate use, the deletion of inaccurate information, and anonymous transactions.[8] For example, if a decision is based on incorrect personal data this could lead to a chain of decisions which need to be able to be followed through from the initial incorrect data.[9] The correction should be made via a notation as adopted in Australian Freedom of Information legislation, rather than by deletion. These issues have been of concern to archivists internationally, and in countries that form part of the European Union in particular, and are discussed further in this paper in relation to current privacy legislative initiatives.[10]

The collection of personal data: the transaction model and privacy protection

One way of looking at the handling of personal data in Privacy Acts within a recordkeeping perspective, is in terms of a transactional model.[11]

In the collection view of personal data, all information passes from one person (natural or corporate) to another. It passes from:

- a data provider to
- a data collector to
- a data controller to
- a recordkeeper.

These terms are used in the OECD *Guidelines on Privacy* and in the *Privacy Act 1988 (Cth)*.

In the transaction model the transmission of data between two parties involves communication between them in the course of transacting 'business'. Each party would keep copies of its outgoing communications as well as the communications it receives from the other party. Each party is both a data provider to the other and a data controller of information provided by the other, all of whom have responsibilities for protecting personal data. The transaction approach makes intentional collection mandatory, which is also implicit in the Privacy Act.[12]

Contextual data (recordkeeping metadata) such as an ID number and other personal identification details that may be kept separately in an electronic system from the informational content gathered on an individual, together comprise identity that 'can reasonably be ascertained' about an individual and which constitute personal information as defined by the Commonwealth, and most Australian Privacy Acts.[13] At the same time the contextual metadata is part of the identity and integrity of the record. The transaction view of privacy highlights time-bound elements of the record essential to its authenticity.

Guidelines on privacy protection for recordkeeping systems

There are good recordkeeping arguments for the protection, as well as the retention of personal data without destruction within a recordkeeping system. Business participants (record creators and keepers), including the professions that are involved in records and information

management, have always had obligations to protect information about individuals in records under statute and common law, which may be distinct from proprietary rights.[14] The protection of privacy is a fundamental principle in recordkeeping practice. Recordkeeping professionals have adhered to principles of confidentiality in relation to records in their custody through their professional codes and through the implementation of access policies which in the public sector have also been legislated in Archival Acts.[15]

Technology can be used to protect personal information without destroying it. For example, *The Recordkeeping Functional Requirements Project* of the University of Pittsburgh proposed in 1991 the notion of 'redactibility', which allows a version of the record that has had the personal data 'removed' to be made available for research, and ensures the integrity of the original record.[16]

Keeping records of who has seen or had access to personal information as a control mechanism over privacy was an outcome of the Independent Commission Against Corruption (ICAC) New South Wales in its Report as implemented in the Road Traffic Authority of NSW.[17] Other design and system features for recordkeeping include rules on access exemptions and privacy protection built into systems at either the transactional or activity level.

In terms of privacy it can be argued that the recordkeeping system if secure, time bound, and linked to retention and access procedures, should provide adequate privacy protection for the record subject, while ensuring that any rights of the record subject are protected without the need to delete the personal information once it has served its purpose.

Recordkeeping issues that have been highlighted by recent privacy legislative initiatives

As stated earlier, the basic principle in all major privacy legislation which conforms with international privacy principles is that personal information should only be collected, used or disclosed for its primary or original purpose, and use and disclosure for secondary purposes is subject to limitations.[18] The question is whether that principle and the limitations it provides are sufficient to satisfy the recordkeeping principle of reliable and authentic records that have other uses not envisaged by their original purpose.[19]

The following questions need to be considered when examining the current privacy legislation:

- Should personal data that identifies the parties to a transaction, which is essential to the reliability of the record and other related personal data that may be held separately in a system or with certification authorities, be de-identified once its 'immediate' use has ceased?
- Should any personal information, which is no longer of immediate use, be de-identified, when it may provide evidence of legal or other abuses?
- Should personal information in both the public and private sector that is more than thirty years old be subject to Privacy laws?
- Should personal information that is inaccurate be destroyed? (Inaccurate information may be unreliable but the record of which it forms a part can still be authentic, if it meets authenticity criteria.)
- Should the right of amendment (and deletion) be separate from access?
- What is role of trusted third parties in protecting privacy?
- Is obtaining the consent of the identifiable person after the 'event' reasonable?
- Should there be more emphasis on the reliability of the record creators?

All of these questions and how they are interpreted impinge on appraisal and disposal recordkeeping best practice, as well as access policy. The impact of privacy principles on current systems in terms of compliance includes obtaining and keeping records of whether

the data subject has been informed of the purpose of collection, or consent for the further use of the personal information collected if needed, and keeping links between the consent and the records themselves. Organisations subject to Privacy Acts will have to guarantee the security of their record and information systems, and have documented retention procedures, which are positive aspects of privacy legislation.

So what is the state of play with privacy legislative initiatives in Australia? We need to look at the range of legislation that provides access to ones' personal information and also protects privacy in relation to the questions raised above.

PRIVACY: THE REGULATORY FRAMEWORK AND AUSTRALIAN INITIATIVES

As a result of the way legislation affecting access and privacy has developed in Australia, privacy law and statutory rights of access to, and protection of personal privacy in government records and some private sector records are found in Freedom of Information (FOI), privacy and archives legislation. It has been very much a patchwork of inconsistent privacy rules for both public and private sector organisations, and now for types of personal information, in particular health, and other 'sensitive' information.

In addition to specific privacy legislation, other legal protection for privacy includes the duty of confidentiality which hinges on a relationship of confidence, and does not die with the confidant. It may be overridden by statutory duties to disclose or public interest disclosure in common law.[20]

The legislative framework: Commonwealth public sector

The *Privacy Act* 1988 (Cth) was originally limited to the Commonwealth public sector, with private sector privacy regulation restricted to consumer credit reporting and separate telecommunications legislation, with all sectors subject to specific privacy rules, in relation to tax file numbers. The Information Privacy Principles (IPP's) that apply to the public sector are based, more or less closely, on the OECD's *Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data* (1980). In 2000 the Act was extended to apply to private sector bodies subject to a large number of exceptions. (The *Privacy Amendment (Private Sector) Act* 2000 is explored later in this paper, see ***RECENT AUSTRALIAN PRIVACY LEGISLATIVE INITIATIVES).***

The intersection of the FOI and the Privacy Act in the Commonwealth is found in the *Freedom of Information Act* 1982, Section 41 which protects privacy in the 'personal information' exemption. 'Personal information' cannot be disclosed when considered *unreasonable* and related to a third party. There is also an amendment right in the FOI Act, that is the right to have incomplete, incorrect, out of date and misleading information corrected in s 47A and 50 (3).[21] The general approach in Australian Privacy Acts has been to create rights in those laws, but to implement them through FOI laws.

Of particular relevance in the light of the argument in this paper on the retention of amended personal information, is S 50, (3) 'To the extent that it is practicable to do so, the agency or Minister must, when making an amendment under paragraph (2)(a), ensure that the record of information is amended in a way that does not obliterate the text of the record as it existed prior to the amendment'.

According to the 1995 Australian Law Reform Commission review of the FOI Act, it was the main vehicle for access and amendment rather than the Privacy Act, and destruction was generally not implemented. The review gave precedence to pressing for access to and protection of medical information, the fruits of which we are now seeing.[22]

Privacy provisions in archival legislation

Commonwealth and most state archival legislation has adequately protected personal information for the lifetime of the person by restricting information that has continuing sensitivity beyond thirty years.

In the initial Commonwealth FOI-Archives-Privacy 'package', the Privacy Act did not extend to records more than thirty years old. In the *Privacy Act* 1988, Section 6 (f), Commonwealth records as defined by subsection 3(1) of the *Archives Act* 1983 that are in the open access period for the purposes of that Act are exempt. Privacy continues to be protected through the *Archives Act* 1983 under s 33 (1) g: 'Information or matter the disclosure of which under this Act would involve the unreasonable disclosure of information relating to the personal affairs of any person (including a deceased person).'[23]

It is important to remember that archival legislation for the public sector is concerned with much more than just access to records. Management and setting standards for quality records, and ensuring their survival are primary objectives.

State legislation and privacy provisions: some recordkeeping issues

There are privacy provisions in all state FOI Acts under 'personal affairs' exemptions. In addition some states have separate Privacy legislation.

Queensland

Queensland has had a Privacy Committee, and Privacy legislation covering credit reporting agencies and listening devices.[24] The *Freedom of Information Act* 1992 in Queensland has an additional regulation that enables Departments to close certain types of records containing personal information permanently. In accordance with this rule, Queensland Health ruled that the Dunwich Benevolent Asylum and similar institutional records are closed forever. Thus medical records from the 1860s that had been opened for years are now closed in response to privacy concerns.[25]

Victoria

There have been many privacy legislative initiatives in Victoria (see ***Victorian legislative initiatives*** below). In recent years a number of amendments to the Victorian FOI Act's personal affairs exemption has taken place, the latest of which provides some additional privacy protection, as well as reversing the mandatory deletions of identifying information about individuals whose identity was not already known to applicants. In the *Freedom of Information (Miscellaneous Amendments) Act* 1999, personal information subject to a request must meet two conditions if a document is to be exempted from disclosure under the *personal affairs* exemption in s 33 (1). Firstly the disclosure of the document must involve information relating to the 'personal' affairs of a person, and secondly, such disclosure must be 'unreasonable'. Any information that identifies a person takes into account any danger to a person in the test of unreasonableness. In addition if the applicant is refused access and has applied for a review of the decision, the agency must give written notice to the persons to whom the information relates, and their rights to intervene in the proceedings.[26]

New South Wales

In NSW there is separate privacy legislation in the *Privacy and Personal Protection Information Act* 1998 which came fully into effect on 1 July 2000, but it applies to the public sector only and excludes state-owned corporations and state investigative agencies.[27] Privacy NSW issues privacy codes of practice for classes of information, an agency or class of agency, or activity, e.g. research, which cover all public sector agencies, including deposited records in archives,

museums etc. (see s 29, (5)). If an agency does not wish to be covered it may seek an exemption, which if granted, requires an alternative code to be approved by the Privacy Commissioner.

In relation to records that are more than thirty years old, a privacy code can extend closure but it must conform to s 52 of the *State Records Act* 1998. In s 29 (3) 'In particular, a privacy code of practice may provide for the protection of personal information contained in a record that is more than 30 years old, and any such provision has effect despite the provisions of any other Act that deals with the disclosure of, or access to, personal information of that kind. Any such code must, to the extent that it relates to personal information contained in a State record that is more than 30 years old, be consistent with any relevant guidelines issued under section 52 of the State Records Act 1998.'

Unlike the Commonwealth Privacy Act where there is an explicit exemption for open period public records, that is records that are more than thirty years old, the NSW Act excludes from its ambit 'information about an individual who has been dead for more than 30 years' in section S.4. 3(a) definition of 'personal information'. This effectively extends the lapse of time for protecting personal information, to a length of time more suitable for medical information than general personal information.

Australian Capital Territory

The *Australian Capital Territory Government Service (Consequential Provisions) Act* 1994 applies the *Privacy Act* 1988 (Cth) to the ACT. There is also a separate *Health Records (Privacy and Access) Act* 1997 (ACT) for the handling of health information (see below for further discussion).

South Australia, Tasmania and Western Australia

South Australia, Tasmania and Western Australia have versions of IPPs as administrative instructions but these do not have the force of law.[28]

RECENT AUSTRALIAN PRIVACY LEGISLATIVE INITIATIVES

***Privacy Amendment (Private Sector) Act* 2000 (Cth)**

Background

On 16 December 1998 the federal Government announced that it intended to legislate to support and strengthen self-regulatory privacy protection in the private sector. The impetus arose from the October 1998 European Union Directive restricting personal information from member countries to other countries unless adequate privacy safeguards are in place and from the need to stimulate confidence in the public to use ecommerce.[29] The outcome has been the *Privacy Amendment (Private Sector) Act* 2000 passed on 21 December 2000 which will come into force on 21 December 2001. The amended *Privacy Act* 1988 continues to cover the Commonwealth and ACT public sector, while each State is expected to have its own Privacy Act for the public sector. However, state/territory bodies that are incorporated companies, societies or associations are deemed to be organisations for the purposes of the Act. By incorporating national privacy principles (NPP's) into the Principal Act, it also regulates how privacy is handled in the private sector. It also gives individuals the right to access and, in some cases amend, their personal records, and the right to make a complaint if they think their information is not being handled properly.

It makes a distinction between personal information and sensitive information, and has separate provisions for health information. Existing data is exempt from some, but not all, of the proposed Act. For example existing information is subject to NPP6 (access and correction rights) only if it is 'used or disclosed'.

Application

The *Privacy Amendment (Private Sector) Act* 2000 extends its ambit to private sector 'organisations' but there are many very significant exceptions. Only 'organisations' that have an annual turnover of more than $3 million are covered, exempting 94% of most businesses *unless they hold health information* other than as part of employer records, and/or collect or disclose personal information for a benefit, service or advantage, that is sell or trade in information.[30] The majority of Australian businesses actually fall within the small business exemption. Exempt small businesses can choose to opt-in and are encouraged to do so. It has been foreshadowed that the Act many need to be amended at a later date to better deal with the complex issues raised by medical information.

S36 insertion 6C Organisations.

What is an **organisation**?

(1) In this Act:

organisation means:

(a) an individual; or

(b) a body corporate; or

(c) a partnership; or

(d) any other unincorporated association; or

(e) a trust;

that is not a small business operator, a registered political party, an agency, a State or Territory authority or a prescribed instrumentality of a State or Territory.

Additional exemptions

- acts of political representatives in relation to electoral matters,
- acts or practices in relation to employee records of an individual if the act or practice directly relates to a current or former employment relationship between the employer and the individual, and
- acts or practices of media organisations in the practice of journalism.

The extra-territorial operation of the Act covers personal information overseas if there is an organisational link with Australia. Contractors to Commonwealth and State agencies are exempted from the private sector NPP's but are bound to public sector IPPs of the Commonwealth or State equivalent laws.

Enforceability

The Act sets out to strengthen the self-regulatory privacy protection introduced in 1998 by the adoption of the *National Principles for the Fair Handling of Personal Information,* with provision for the development of industry and business codes of practice that have legislative force and their own complaint handling regime that are consistent with the standards to be laid down in legislation. An industry code has to be approved by the Privacy Commissioner (they are not a disallowable instrument and therefore not subject to the scrutiny of Parliament), and must specify the organisations bound to it. It sets up a default legislative regime if there is no approved code or a complaint handling body and a code adjudicator. The Privacy Commissioner investigates complaints (where there is no code adjudicator), as under the New South Wales and Victorian Privacy Acts. Determinations made by a complaints handling body or Privacy Commissioner are enforceable in the Federal Court or Magistracy (but their enforcement requires a 'de novo' or further hearing, and facts could be challenged).[31]

Whether the amendments will lead to powerful industries dominated by large companies setting up their own complaints handling bodies to their own advantage, as well as a plethora of different codes, remains to be seen. However it is unlikely that any major changes to the Act will take place in the near future.

Recordkeeping Issues re: Privacy Amendment (Private Sector) Act 2000

From a recordkeeping view as articulated in this paper, identifiable personal information within a business transaction, either in relation to parties to a transaction or record subjects, or other third parties who may also hold authentication information, are elements of identity essential to the reliability and authenticity of the record both at the time of creation and over time. The following section considers the impact of the *Privacy Amendment (Private Sector) Act* 2000 in relation to records over time.

Archival exemptions

A record in the principal *Privacy Act 1988* is defined very broadly:

Subsection 6 (1)

record means:

(a) a document;

(b) a database (however kept); or

(c) a photograph or other pictorial representation of a person;

but does **not include:**

(d) a generally available publication;

(e) anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition;

(f) Commonwealth records as defined by subsection 3(1) of the *Archives Act 1983* that are in the open access period for the purposes of that Act;

(fa) [see below]

Privacy Amendment (Private Sector) Act 2000, S 25 Subsection 6(1) (after paragraph (f) of the definition of *record*)

Insert: or

(fa) records (as defined in the *Archives Act 1983*) in the custody of the Archives (as defined in that Act) in relation to which the Archives has entered into arrangements with a person other than a Commonwealth institution (as defined in that Act) providing for the extent to which the Archives or other persons are to have access to the records; or ....

Commonwealth records continue to be specifically exempted from the legislation if they are in the open access period and therefore not necessarily in archival custody, (see definition of records in open access period in s3 (7) of the *Archives Act* 1983, that is 'a record is in the open access period if a period of 30 years has elapsed since the end of the year ending 31 December in which the record came into existence'). Distributed custody or distributed management, that is electronic records that may never be physically transferred to an archival agency even if they are under the legal custody of the archives, would be covered.[32] In the Amendment Act in s 25 Subsection 6(1) after paragraph (f), insert (fa) there is an added exemption to cover records, other than Commonwealth records, which the National Archives of Australia (NAA) may arrange custody and access to for the Archives or other persons. Records (as defined in the *Archives Act 1983*) in the custody of the Archives (as defined in that Act) relate

to records of Parliament and the courts (see s 21 *Archives Act 1983*). As pointed out in the submission to the Attorney General from the Australian Society of Archivists and the Australian Council of Archives, in January 2000, there is no exemption for records in a private archive or a business wishing to provide access to older records containing personal information.[33] Presumably the assumption behind this exclusion is that these records will have been de-identified or destroyed well before they are thirty years old.

One suspects that the traditional lack of statutory rights of access to private records has inadvertently brought about the anomaly in the treatment of private as opposed to public records. In the private sector access to records has been based on property concepts. The kind of exemption developed for public records at the federal level has not been included for private sector organisations under the amendments to the Privacy Act.

Schedule 3 National Privacy Principles, Privacy Amendment (Private Sector) Act 2000: Recordkeeping concerns

The Australian Society of Archivists and the Australian Council of Archives (ASA/ACA) in their submission to the Attorney-General's Department in relation to the Commonwealth Privacy Amendment Bill, identified Principle 1 and 2 (in particular), and 3, 4, 6, 9, and 10 as of concern in the context of transfer of and access to personal information in private records held in a private deposit archives.[34] The archival notion of 'lapse of time', which varies for categories of records has been one of the major arguments supporting the eventual disclosure of personal information to third parties. More importantly if records are destroyed or de-identified they are unlikely to reach an archive or be available for future research. Access has always depended on disposal practices. Apart from the effect on future research, NPP 2, NPP 3, and 6 encourage indirectly, and NPP 4 and 10.4 directly the early destruction of personal information that may be relevant to the reliability of the transaction, and the transacting parties, and limit evidence of rights and entitlements of participants. (See ***Health Information: legislative Initiatives*** for a discussion on 10.4.)

The NPPs (paraphrased below) that encourage the early destruction of personal information are:

NPP2 Use and disclosure

It makes it illegal to use personal information for anything other than the primary purpose of the information collection except for certain permitted secondary uses which include when the secondary purpose is related to the primary purpose, a disclosure avoids a harm, where authorised by law, public interest circumstances or with the consent of the individual.

(Cth, NSW and Vic have similar requirements)

The ASA/ACA submission had argued that the Amendment Act would make it illegal to use personal information for anything other than the primary purpose of the information collection without the consent of the individual, and would also encourage the early destruction of records that have served their primary purpose. There is however a long list of exemptions in NPP2 to the general requirement of use for primary purposes only, although none of them relate to general access for research purposes.[35]

A commercial transaction could trigger a number of activities or purposes. What is the primary purpose, and when does it finish? Circumscribing the boundary of the primary purpose of a record is a business choice. A private organisation (e.g. a not-for-profit archival collecting body) could argue that its primary purpose is collection of, and provision of access to personal information. It could also interpret the objects clause, as a recognition to retain personal information in the context of 'business' using professional recordkeeping principles and best practice.

Privacy Amendment (Private Sector) Act 2000, **3 Objects**

(b) (iii) recognises important human rights and social interests that compete with privacy, including the general desirability of a free flow of information (through the media and otherwise) and *the right of business to achieve its objectives efficiently.*

An archive that comes under the small business operator exemption (*Privacy Act 1988, as amended in* 2000, 6D Small business and small business operators) may lose its exempt status if it falls into the category of an organisation that:

(4)

(c) discloses personal information about another individual to anyone else for a benefit, service or advantage; or

(d) provides a benefit, service or advantage to collect personal information about another individual from anyone else.

If a large business archive or business organisation (which is not an exempt organisation) provides access to personal information that is even fifty years old it may be in breach of NPP 2.1, use and disclosure for secondary purposes if it fails the 'reasonable expectations' test, or the persons concerned have not consented to further uses. They could use NPP 2.1, (d), (i) which provides an exemption if 'it is impracticable for the organisation to seek the individuals consent before the use or disclosure'.[36]

However in the *Privacy Amendment (Private Sector) Act 2000* s 16 c limits the application of some principles to after the commencement of the Act including NPP 2[37] so that at least personal information already held by an organisation does not need retrospective consent from the data subjects for other uses, subject to any other statutory restrictions. Personal information collected after the commencement of the Act would be subject to all the NPP's if collected by an organisation as defined by the Act.

NPP 3 Data quality

An organisation must take reasonable steps to make sure that the personal information it collects, uses or discloses is accurate, complete and ***up-to-date.***

Principle 3 so far as it relates to personal information used or disclosed, applies to previously collected personal information. Accuracy is dependent on reliable authors (identity) and a complete record depends on its integrity.

NPP 4 Data security

Data no longer needed for any authorised purpose in the organisation must be destroyed or permanently de-identified.

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 National Privacy Principle 2.

(Cth, NSW and Vic have similar requirement)

Although privacy advocates argue that the destruction principle can be avoided by finding secondary uses, it will be attractive to those avoiding access requests.[38] NPP 4 applies to previously collected personal information. It relates to the integrity and identity of the record.

NPP 6 Access and correction

6.5 If an organisation holds personal information about an individual and the individual is able to establish that the information is not accurate, complete and up-to-date, the organisation

must take reasonable steps **to correct the information so that it is accurate, complete and up-to-date.**

It does not state here that the information has to be destroyed but read with NPP4 it can be interpreted to encourage early destruction. As stated earlier, this principle interacts with Freedom of Information laws, and the exemptions in these laws that protect privacy are generally applied.[39] Again it relates to integrity and identity of the record.

(Cth, NSW and Vic have similar requirement)

NPP 7 Identifiers

Organisations must not use as their own identifiers any personal identifiers assigned by the Commonwealth government agencies, and must not use or disclose such identifiers (with exceptions)

Certification authorities (CA'S) would be limited in how they use or disclose at least some identifiers which they would have a primary purpose in collecting.

NPP 8 Anonymity

Wherever it is lawful and practicable, individuals must have the option of not identifying themselves when entering transactions with an organisation.

There are some transactions where anonymity may be desirable. For recordkeeping purposes identification of the parties to the transaction is needed for reliability purposes. While 8 is of concern it does have a proviso that would make it apply only when it is not legally necessary to be identified. Pseudonyms have been suggested as a preferable principle to anonymous transactions as CA's can hold the real names separately to prevent their disclosure.[40] The option to remain anonymous when entering transactions, (NPP 8) and transfers of personal information out of Australia (NPP9), have an exemption that would satisfy archival concerns that fall into this category, that is 8 (ii) 'it is impracticable to obtain the consent of the individual to that transfer' they would not be required to do so.

VICTORIAN LEGISLATIVE INITIATIVES

In 1998-9 a Victorian Privacy Bill was proposed to cover both the public and the private sector in the context of ecommerce developments.[41] It did not proceed. However more recent initiatives have led to the *Information Privacy Act* 2000 (Vic) which was passed on the 30 November 2000, and comes into force on 1 September 2001. It adopts a set of Information Privacy Principles which are based on the National Privacy Principles set out in the *Privacy Amendment (Private Sector) Act 2000* (Cth).

Information Privacy Act 2000 (Vic)

Application

The Act imposes privacy obligations in respect of the management of personal information across the Victorian public sector, that is state government agencies, and includes state owned enterprises, local councils and Members of Parliament. It applies to personal information, and exempts generally available publications.

The Victorian Act has many similar provisions and definitions to the Federal Act; the IPPs are based on the NPPs, which contribute to national legislative consistency. The NSW Privacy Act adopted its own version of them. The recordkeeping issues are therefore the same as those noted above. Important features are:

- It excludes the private sector (which is covered by the Commonwealth's Privacy Act as amended).
- It allows for codes of practice that cannot be less stringent than those in the Act (as in Commonwealth).
- It adopts an onward transfer principle to limit the transfer of information to recipients bound by similar privacy obligations.
- It adopts the definition of 'organisation' to cover persons and organisations.
- It provides for access to personal information by the data subject.

Archival exemptions

Unlike the Commonwealth Privacy Act, not-for-profit archival bodies are specifically exempted, although property language is not completely avoided. See s 11. Publicly-available information.

(1) Nothing in this Act or in any IPP applies to a document containing personal information, or to the personal information contained in a document, that is—

(a) a generally available publication; or

(b) kept in a library, art gallery or museum for the purposes of reference, study or exhibition; or

(c) a public record under the control of the Keeper of Public Records that is available for public inspection in accordance with the Public Records Act 1973; or

(d) archives within the meaning of the Copyright Act 1968 of the Commonwealth.

(2) Sub-section (1) does not take away from section 16(4) which imposes duties on a public sector agency or a Council in administering a public register.

COPYRIGHT ACT 1968 SECT 10

Part II—Interpretation 10 Interpretation

archives means:

(a) archival material in the custody of:

(i) the Australian Archives;

(ii) the Archives Office of New South Wales established by the Archives Act 1960 of the State of New South Wales;

(iii) the Public Record Office established by the Public Records Act 1973 of the State of Victoria; or

(iv) the Archives Office of Tasmania established by the Archives Act 1965 of the State of Tasmania; or

(b) **a collection of documents or other material to which this paragraph applies by virtue of subsection (4).**

(4) Where:

(a) a collection of documents or other material of historical significance or public interest that is in the custody of a body, whether incorporated or unincorporated, is being maintained by the body for the purpose of conserving and preserving those documents or other material; and

(b) the body does not maintain and operate the collection for the purpose of deriving a profit;

paragraph (b) of the definition of archives in subsection (1) applies to that collection.

HEALTH INFORMATION: LEGISLATIVE INITIATIVES

Are certain matters more private and more sensitive than others? Is health information more sensitive than other information? It has always been treated as a special case. The NPP's in the *Privacy Amendment (Private Sector) Act* 2000 (Cth) have specific provisions regarding limits on the *collection* of sensitive data categories, which include health information. There are no special restrictions on the *use or disclosure* of sensitive information, except for health data. In addition the NPP's apply generally to health information as personal information. The NSW Privacy Act also includes a sensitive data principle which includes health information and imposes tighter conditions on disclosure but not on collection or use.[42] The *Information Privacy Act* 2000 (Vic) excludes health within its sensitive data principle, because it is covered in the Health Records Act (see below).

A major development that has implications for health privacy is the move of health information online. A national network, potentially feeding into international health networks, with a single electronic medical record which will link the patient, hospitals and doctors, crossing over the public-private divide and state jurisdictions, has huge privacy implications.[43] The storage and retention of the networked patient records, their reliability and authenticity crucial to their trustworthiness and probative value, have not been fully addressed by any Australian health privacy legislative initiatives.

Health Records (Privacy and Access) Act 1997 (ACT)

The Australian Capital Territory was the first Australian jurisdiction to legislate for the right of patients to have access to *both public and private health records.* The precise coverage of the law depends on the interaction of several key definitions, such as *health service provider, health record,* and *personal health information.* While health service providers such as doctors, hospitals and clinics are subject to the Act in relation to all health records, any other organisation or individual is also covered in respect of any personal health information they hold. Employers and insurance companies, for example, are subject to the law in relation to any information about an individual's 'health, illness or disability' that they may hold for whatever purpose.

In relation to its recordkeeping elements, the Act is a preferable model to the Commonwealth and the Victorian Privacy Acts. It presents a practical compromise between a general requirement for accuracy and a recognition of the need for a complete historical record. Principle 7 provides for a record found to contain inaccuracies to be held separately from the 'active' record in use by the treating team.[44]

Privacy Amendment (Private Sector) Act 2000: health provisions

The Commonwealth health provisions have to be read in conjunction with NPP 10 sensitive information, of which they form a part, and in particular NPP 10.2 - 10.4. The Act adheres to a view of strict medical confidentiality.

Privacy Act 1988, as amended in 2000.

6 Interpretation
sensitive information means:

(a) information or an opinion about an individual's:

.....

(b) health information about an individual.

health information means:

(a) information or an opinion about:

(i) the health or a disability (at any time) of an individual; or

(ii) an individuals expressed wishes about the future provision of health services to him or her; or

(iii) a health service provided, or to be provided, to an individual;

that is also personal information; or

(b) other personal information collected to provide, or in providing, a health service; or

(c) other personal information about an individual collected in connection with the donation, or intended donation, by the individual of his or her body parts, organs or body substances.

Note: The definition covers both information handled by a health service provider AND other organisations, e.g. insurers.

health service means:

(a) an activity performed in relation to an individual that is intended or claimed (expressly or -otherwise) by the individual or the person performing it:

(i) to assess, record, maintain or improve the individuals health; or

(ii) to diagnose the individuals illness or disability; or

(iii) to treat the individuals illness or disability or suspected illness or disability; or

(b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

The boundary of the medical record is problematic although the definition of a health service in the Act provides an activity-based definition that is useful in the electronic context. The distinction is made between the information of health service providers and other organisations' health information. The issue of the reliability of the health care providers is not addressed, which is central to the reliability of the health content. Health service providers are not specifically defined (despite an earlier Attorney General Draft Provision to that effect); instead they are an 'organisation' which includes an individual that provides a health service.

Permanent de-identification of health information before disclosure rather than a 'redacted' version applies to an organisation that collects health information. NPP 10.4 states that 'If an organisation collects health information about an individual in accordance with subclause 10.3, the organisation must take reasonable steps to **permanently de-identify the information before the organisation discloses it**'. NPP 10.2 deals with the collection of health information as part of a health service, that is 'the patient record' and is not subject to NPP 10.4 (see the Victorian Health Act which also distinguishes between the health provider's record and other organisations' health records).

Health Records Act 2001 (Vic)

The *Health Records Act* 2001 (Vic), was passed on the 10 April 2001 and comes into force from 1 July 2002 unless proclaimed earlier. It aims to protect the privacy of individuals' health information through privacy standards for the handling of health information (including information collected in providing a health, mental health, disability, aged care or palliative care service) with eleven health-specific privacy principles. Health information was excluded from the operation of the Victorian *Information Privacy Act* 2000 (although not the Commonwealth one). It also provides individuals with an enforceable right of access to their own health information contained in a 'document' (as defined in the *Interpretation of Legislation Act* 1984, s 38), and a framework for the resolution of complaints regarding the handling of health information. The principles in practice also place some limit on the rights of individuals in relation to access to their personal health information, but denial will be limited to specified exemptions.

Application

The Act applies to any Victorian business (profit and not-for-profit, incorporated and unincorporated,) or person (see Division 1 and 2, Part 2) that *collects, holds or uses health information*, and would therefore include the archive of a public or private hospital. Access to health information in the public sector continues to operate through *Freedom of Information Act* 1982, (see *Health Records Act 2001* (Vic), s 16), but the former has been amended by the Health Records Act so that s 33 provides the same reason for refusing access in both acts, that is there has to be a serious threat to the life of the person making the request.[45] Existing law on confidentiality and access rights in statutes will not be overridden by the Act, (s 7 and 27) and the Act operates concurrently with Commonwealth laws (s 8), as long as they are not inconsistent with the Commonwealth Act. The extent of the overlap of provisions dealing with access to and handling of personal health information in the private sector in Victoria with the Commonwealth's Privacy Amendment Act's health provisions will also need to be resolved.[46]

Archival exemptions

Like the *Information Privacy Act* 2000 (Vic), s 15 provides for a public record under the control of the *Public Records Act* 1973 and not-for-profit archival bodies to be specifically exempted from the Act. S 95 (1) ensures that the Act applies to a deceased individual who has been dead for 30 years or less, in practice bringing it in line with the standard medical record closures followed by archival organisations, and which the NSW Privacy Act applies to all personal information (see above).

Recordkeeping issues

The Victorian Act contains a number of recordkeeping issues that still need to be resolved. The Act acknowledges that health information will be held by a number of health service providers and organisations, including health information in employment records or schools. Health information has to also be personal information as defined in the Act (i.e. non-health personal information in health organisations is exempted from this Act) in Victoria.[47] The distinction between ownership and access is upheld, which complies with existing property concepts (see s 5 When does an organisation hold health information?).

As in the Commonwealth legislation, there is a distinction made between health information held by a service provider and that held by other organisations. HPP 4.2 Data security and data retention, provides that a health service provider must not delete health information relating to an individual, even if it is later found or claimed to be inaccurate, unless, permitted by law, or not contrary to a law. Health service providers' records have specific retention guidelines. Information can be deleted related to a child once the individual attains twenty five years, or in any case seven years after the last occasion on which a health service was provided to the individual. Does the seven years apply to discrete data or the patient's whole record or history? How is this reconciled with a longitudinal collection of information about a person's health needed for life long care?[48] A business activity involves a series of transactions that record 'what happened'. A doctor may record a series of visits, episodes, or 'events'; it is the series of events that is the history of the patient, and needs to be viewed as a whole.

HPP 4.5 relates to health information in organisations other than Health service providers, and follows the Commonwealth and Victorian Information Privacy Acts that make it necessary to destroy or permanently de-identify health information in organisations which is no longer needed for the purpose for which it was collected.

The piecemeal and inconsistent jurisdictional approach to privacy and health will be challenged by a national health network which will require consistent principles, and the retention of health information for at least the lifetime of the patient.

CONCLUSION

Privacy protection in the online environment is crucial, and legislative action in this area is most welcome. However the current legislation contributes to a patchwork approach. It is difficult to reconcile the amendments to the Federal Privacy Act in particular, with notions of public interest in disclosure, and long term retention for research purposes, which take into account the integrity of record over time, found in the broader privacy regulatory framework which has included FOI and archival legislation. The new privacy legislative initiatives may in fact 'legalise' some unacceptable recordkeeping practices, including encouraging the early destruction of personal information no longer required for immediate use, or its de-identification.

If records are handled by professionals (business and recordkeeping), that understand both their legal and ethical duties, and as confidential relationships, privacy is much more likely to be protected than by legislation that exempts powerful interest groups such as the media and allows the government to legislate which agencies are exempt from the Privacy Act. Other trusted third parties, from archival authorities to professional and industry regulators, as well as the users, contribute to the web of trust that protects personal information.

Technology (e.g. encryption, rights management systems), and mediated trust (business and recordkeeping professionals and other trusted third parties), can support privacy based on recordkeeping principles that keep, rather than de-identify the metadata relating to the author, recipient and/or record-subjects so that the transactions remain reliable and authentic. The right of access to personal information needs statutory backing; however the accuracy of the information depends on reliable record creators, and keeping the metadata that identifies their professional competencies and their delegations. In the online environment the identity of the record creators also provides trust and legal validity to the content of the business transaction.

ENDNOTES

* I acknowledge the helpful guidance from Moira Patterson, Senior Lecturer, Faculty of Law, Monash University on alerting me to recent changes to the Privacy and FOI law. However the legislative interpretation is the author's alone and is not meant to provide legal advice on the matters herein. *Note: The legislation is stated as at 1 June 2001.*

1 *Business* is defined in this paper in the very broadest sense to encompass social and organisational activity of all kinds.

2 The implications of privacy protection in records over time are rarely addressed outside of the information and records communities.

3 From within the 'records continuum model' the identity of recordkeeping participants is found on the identity axis, at all four dimensions, as necessary for the creation, capture, organisation and access over time to records. See Frank Upward, 'Structuring the Records Continuum, Part One: Postcustodial Principles and Properties' *Archives and Manuscripts*, Vol. 24, No. 2, Nov.1996, p. 278.

4 Heather MacNeil, *Trusting Records, Legal, Historical and Diplomatic Perspectives,* Kluwer, Dordrecht, 2000, p. xi. Elements of record trustworthiness are explored through law, archival science and history. MacNeill concludes that while the technological means of assessing and ensuring record trustworthiness have changed fundamentally over time, the underlying principles have remained remarkably consistent.

5 The *International Research on Permanent Authentic Records in Electronic Systems (InterPARES) Project* is defining record authenticity in terms of the attributes that establish its identity and integrity. See Authenticity Taskforce documents at http://www.interpares.org

6 InterPARES is proposing that degrees of record authenticity can be presumed if benchmark requirements have been met by the record creators that also take account of the needs of the legal system, with additional verification undertaken by the preserver where these requirements appear insufficient to presume authenticity. The more requirements that are satisfied, the more probable is authenticity. See 'Draft Requirements for Ensuring Authenticity of Electronic Records Over Time', The InterPARES Project, Authenticity Task Force, version 2.1, May 2001 (Working Document: not available publicly). Note: InterPARES shifts responsibility for protecting the record's authenticity over time from the *creator* to the *preserver*, i.e. a neutral third party, usually an archival authority, once the business purposes of the records have been exhausted. The findings of the Authenticity Task Force to date are analysed by Heather MacNeil in, 'Providing Grounds for Trust: Developing Conceptual Requirements for the Long-Term Preservation of Authentic Electronic Records', *Archivaria,* Vol. 50, 2001.

See also ISOTC 46/SC 11 N253, ISO/DIS 15489, 29 May 2000 *Records Management Standard* (Draft), definitions: 7.2.2 Reliability; 7.2.3 Integrity; 7.2.1 Authenticity.

[7] The Covenant is an international instrument based on the 1948 directive of the United Nations' *Universal Declaration of Human Rights*, Article 12.

[8] The 'deletion principle' is found in the *Australian Privacy Charter*, and in the Attorney General's Report of 1996 to the Privacy Commissioner who recommended it be added to the existing privacy principles. It appears in the current Commonwealth *Privacy Act 1988*, as amended, in NPP 4.2.

[9] Danielle Laberge, 'Information, Knowledge and Rights: The Preservation of Archives as a Political and Social Issue', *Archivaria*, Vol. 25, Winter, 1987-88, pp. 44-50. This article focuses on a case study detailing the destruction of young offenders' judicial files to protect their privacy, which led to lack of evidence of their mistreatment. The assessment of programs and the potential abuse of individuals require the retention of personal data, at least for the life of a person, in order to redress both individual and collective wrongs.

[10] In Sweden the *Personal Data Act* 1998 (conforming to the European Union Data Protection Directive) replaced the *Data Act 1973*. The processing of data that has been collected before the new Act came into operation is regulated by the 1973 Act. In the *Personal Data Act* 1998, section 3, under 'term', personal data is defined as 'all kinds of information that directly or indirectly may be referable to a natural person who is alive'. There is also a specific provision to allow personal data to be retained for longer than necessary for its original purposes. Section 9 states that 'Personal data may be kept for historical, statistical or scientific purposes for a longer time than stated in the first paragraph i). Para (i) states that 'personal data is not kept for a longer period than is necessary having regard to the purpose of the processing'.

[11] I would like to acknowledge Chris Hurley for the useful distinction that he made between transaction and collection privacy models while giving guest lectures at Monash University in the Bachelor of Information Management in 1996.

[12] According to Graham Greenleaf the intentionality element in record creation is implicit in the *Privacy Act 1988* (Cth). See Graham Greenleaf, 'Privacy Principles: Problems in Cyberspace - Likely Areas of Controversy and Interpretation', in Papers from *The New Australian Privacy Landscape*, Faculty of Law, Continuing Legal Education, The University of New South Wales, 14 March 2001, p. 3.

[13] Even in paper recordkeeping systems, personal data that would further identify an individual may be found in related control records, and not on the face of the record. It is the linking at the system level that may infringe personal privacy. See also Greenleaf, 'Privacy Principles: Problems in Cyberspace', *op. cit.*, p. 9, and the definitional problem of 'personal information' that should take other sources into account than what is immediately apparent. Greanleaf in fact suggests a definition based on interactions of individual communications which is a transactional view, *ibid*, p 11.

[14] These obligations are found in a series of Acts established under Freedom of Information, privacy, recordkeeping legislation and the common law, which include access rights and restrictions, accountability mechanisms, and rights of appeal.

[15] *International Code of Ethics for Archivists*, Code 7, 'Archivists should respect both access and privacy, and act within the boundaries of relevant legislation' adopted by the General Assembly, International Council of Archives in its XIIIrd session in Beijing (China) on 6 September 1996 http://www.ica.org/c_ethics_e.html

[16] University of Pittsburgh, School of Information Science, *The Recordkeeping Functional Requirements Project* at http://www.lis.pitt.edu/~nhprc 1 requirement 13, 'Redactable'.

[17] Independent Commission Against Corruption, NSW *Report on Unauthorised Release of Government Information*, Sydney, ICAC, 1992, 3 vols, in which Commissioner Temby attributed poor recordkeeping as a factor in corrupt practices uncovered. 'Following the investigation of ICAC into the sale of personal information stored in DRIVES' predecessor system, (Roads & Traffic Authority NSW records management system) DRIVES itself was constructed so that all views of the records are logged with the user Id and time and date-stamped. All transactions are created with user Id and time and date-stamp. No records may be deleted, only corrected by a new record which is logged with the user details. You cannot call up any DRIVES record without creating a record of the view transaction. While the transactional records are almost entirely electronic, the source documents for the transactions are retained to provide a means of checking what is in the system. This does not prevent improper access; it simply provides a means of auditing access which can be matched to the users' work documentation to identify any view of the records which cannot be accounted for. Audits of DRIVES transactions are conducted in all motor registries every year. When the auditors turn up, they go through the previous six weeks of work to look for anomalies. It's not foolproof but it was designed with the intention of providing a reasonable protection for the personal information held in the system. This is required specifically under the legislation (the Road Transport (Driver Licensing) Act 1998 (sections 12, 40 & 41) and the Road Transport (Vehicle Registration) Act 1997 (section 11). It is supported by training which emphasises the requirement not to give out personal information.' Source: Personal communication to the author from Anne Picot, Corporate Archivist, Roads & Traffic Authority NSW, 1 June 2001.

[18] The principle, ('Purpose Limitation Principle') that personal information should only be used or disclosed for its primary or original purpose addresses the objective of Articles 6 (1) (b) and 7 of the European Directive of Privacy 95/46. See Nigel Waters, 'A Comparative Analysis of Australian Privacy Laws with Special Reference to the Concept of "adequacy" for the Purposes of the European Union Data Protection Directive', in Papers presented to *The New Australian Privacy Landscape*, Faculty of Law, Continuing Legal Education, The University of New South Wales, 14 March 2001, (no pagination).

[19] See John Miller, 'Settling Accounts with a Secret Police: the German Law on the Stasi Records', *Europe-Asia Studies*, Vol. 50, No. 2, 1998, pp. 305-350. Miller's article provides an analysis of why the records of a highly intrusive personal nature were not destroyed after German re-unification but rather covered by specific legislation passed by the Federal German government in order to carry out 'corrective justice' through the legal system. The German experience in handling

the records of individuals of the State Security Service of the former German Democratic Republic (STASI) is instructive. The German Law on the STASI records justified their retention for the purpose of 'settling the accounts' with the former East German regime through the judicial system, despite the fact that the personal information had been gathered 'illegally'. At the same time the Law protected the privacy interests of the victims of the STASI surveillance. Australian cases of 'illegally' gathered personal information include the NSW Special Branch files on prominent lawyers, politicians, and civil libertarians. These files were destroyed notwithstanding their potential value as judicial evidence. The 'Heiner affair' in Australia is another example of 'legal destruction' of records related to an aborted inquiry into the John Oxley Centre, Wacol, Queensland and its manager which included evidence of child abuse. See, Chris Hurley, 'The Heiner Shredding: An Appreciation', http://www.caldeson.com/RIMOS/heiner.html, accessed June 2001.

[20] In a 1999 English Court of Appeal case, *Source Informatics Ltd* requested permission from the Department of Health to allow general practitioners and pharmacists to provide it with statistical information on their prescribing habits extracted from patient data, and provided to the company in de-identified form, in order to sell this information to drug companies. The request was dismissed on the grounds that the disclosure would be a breach of confidentiality even if the data were de-identified, unless *Source Informatics Ltd* could demonstrate a high public interest value in the disclosure, for example for medical research. As the disclosure was not found to be in the public interest the application for judicial review was dismissed. If the English case is followed, a confidential relationship at least between a health care provider and patient, continues to protect patient information from third party disclosure, where a patient has not consented to other uses, unless there is a demonstrable public interest in its disclosure. Whether or not the data is de-identified the potential harm to the patient arises from the breach of trust caused by the lack of consent for uses of personal information other than that for which it was intended. See *R v Department of Health Ex Parte Source Informatics Ltd,* [1999] 4 All ER 185, in Medical Law Reporter, *Journal of Law and Medicine,* Vol. 8, Aug. 2000, pp. 27-30.

[21] It was recommended that s 47A and 50 (3) of the *Freedom of Information Act* 1982 (Cth) be repealed when the *Privacy Act* 1988 first came into effect but this never happened.

[22] Australian Law Reform Commission, Report 77, *Open Government: a Review of the Federal Freedom of Information Act 1982,* Australian Law Reform Commission, Administrative Review Council, Australian Government Publishing Service, Canberra, 1995.

[23] The 1997 ALRC review of the *Archives Act* 1983 envisaged a different personal affairs exemption based on a universal actual harm test. It reluctantly recommended a change from 'personal affairs' to 'personal information the disclosure of which would, or could reasonably be expected, to have an adverse effect on any person', to align it with the Privacy and FOI Acts. See Law Reform Commission, Report No. 85, *Australia's Federal Record,* 1998, Commonwealth of Australia, Canberra, p. 297.

[24] *Invasion of Privacy Act* 1971 (Qld)

[25] As reported on the Aus-archivists listserv in March 2000. Personal health records would normally be closed for 100 years from date of creation in most public archival institutions.

[26] Under earlier amendments made in Victoria in July 1999, the Kennett government's *Freedom of Information Amendment Act* 1999, Part 3 A required the deletion of any identifying information relating to a person subject to a request, including any public officer involved in actions related to the request, whose identity was not already known to an applicant. This was the government's response to a Victorian Civil and Administrative Tribunal decision that information was not personal when used in the context of an officer's duties (i.e. employees). See *Re Coulston and Frankston Hospital* 2 November 1998, in which the names of nurses on duty at Frankston Hospital on a particular day were disclosed to a convicted murderer as a result of the VCAT decision. The convicted murderer sought them in an attempt to get evidence to support his alibi that he was visiting his wife in hospital at the time when the murders took place. These amendments have since been reversed. See Moira Patterson, 'Victoria's New FOI Bill some long overdue reforms but still room for improvement', *FOI Review,* Dec. 1999, Vol. 84, pp. 90-93 and Jason Pizer, 'Putting the 'O' back into FOI' *Law Institute Journal,* March 2000, pp. 63-66.

[27] See also Graham Greenleaf, 'A New Era for Public Sector Privacy in NSW', *Privacy Law & Policy Reporter,* Vol. 5 No 7, February 1999. http://www2.austlii.edu.au/~graham/cyberspace_law/NSW_Act.html

[28] Waters, 'A Comparative Analysis', *op. cit.*

[29] It has been an important business risk in that Australia's privacy laws had not conformed to the 1995 European Directive on Privacy which does not allow personal data to be transferred to a non-EU country that cannot ensure an adequate level of privacy protection. In relation to ecommerce aspects of privacy, see 'Ministerial Declaration on the Protection of Privacy on Global Networks', OECD Conference, *A Borderless World: Realising the Potential of Global Electronic Commerce,* Ottawa, 7-9 October 1998.

[30] The remaining 6% of businesses are responsible for 70% of total sales of Australian businesses. Data from House of Representative, Standing Committee on Legal and Constitutional Affairs, *Advisory Report on the Privacy Amendment (Private Sector) Bill, 2000,* June 2000, para 2.20.

[31] A right of appeal from the decisions of Code Adjudicators to the Privacy Commissioner was added to s. 18B1. Waters, *op. cit.,* 'A Comparative Analysis'.

[32] In March 2000 the National Archives of Australia announced that it accepts custodial responsibility for Commonwealth records, in all formats, that have been selected as national archives. Custody would not have had to be requirement for Subsection 6(1) after paragraph (f) to apply to open period Commonwealth records. In any case 'temporary Commonwealth records' that remain with agencies for lengthy periods, and contain personal information, could avail themselves of this subsection. http://www.naa.gov.au/recordkeeping/custody/summary.html

[33] The Commonwealth Privacy Amendment Act 2000 should at least have adopted the definition of archives in the *Copyright Act* 1968 to extend an exemption to archives of 'not-for- profit' organisations, as in fact the Victorian *Information Privacy Act* 2000 s 11 (1) (d) and *Health Records Act* 2001 (Vic) s 15 have done.

[34] The Australian Society of Archivists and the Australian Council of Archives (ASA/ACA), *Submission to the Attorney-General's Department in relation to the Commonwealth Privacy Amendment Bill*, ASA Bulletin, No. 1, January 2000. With the large number of exemptions to private sector organisations in the Privacy Amendment *(Private Sector)* Act 2000 the concerns expressed by the Australian Society of Archivists and the Australian Council of Archives (ASA/ACA), are for the moment less pressing than they originally appeared.

[35] *Privacy Act* 1988, as amended, Part VI Division 2 does allow for the Privacy Commissioner to make a Public Interest Determination allowing for derogation from an NPP which could be requested for particular records.

[36] Consent of the individual is generally given a wide scope of interpretation according to Waters, 'A Comparative Analysis', *op. it.*

[37] See s 16 C (1A) 'National Privacy Principle 2 applies only in relation to personal information collected after the commencement of this section.' *Privacy Amendment (Private Sector) Act* 2000 limits the application of some principles to after the commencement of the Act including NPP 1, 2, part of 3, 6, 8, and 10.

[38] Greenleaf, 'Privacy Principles: Problems in Cyberspace', *op. cit.*, p. 6

[39] Waters states in 'A Comparative Analysis', *op. cit.*

[40] Greenleaf, 'Privacy Principles: Problems in Cyberspace', *op. cit.*, p. 7.

[41] State of Victoria, Department of State Development, Multimedia Victoria 21, *Discussion Paper, Information Privacy in Victoria: Data Protection Bill, Discussion Paper,* July 1998.

[42] *Privacy and Personal Information Protection Act 1998*, (NSW), s 19(1).

[43] *Health Information Network for Australia: Report to Health Ministers by the National Electronic Health Records, Taskforce* Commonwealth of Australia, July 2000. http://www.health.gov.au/healthonline/ehr_rep.htm

Darren Gray, 'Electronic health records unveiled', 2000-09-22 00:42:28, The Age.

http://www.theage.com.au/cgi-bin/printversion.pl?story=20000922/A11533-2000Sep21

[44] Nigel Waters 'New health privacy law in Canberra', *Privacy Law & Policy Reporter*, Vol. 4, 1998, p. 121.

[45] Elizabeth Armstrong, 'Access to Medical Records: An Update', *Law Institute Journal,* June 2001, p. 63.

[46] 'Some States have enacted legislation, for example the *Victorian Health Records Act* 2001 (Vic), which applies to health care professionals, whose services are regulated under State law. Unless the constitutional validity of the Commonwealth's privacy provisions in relation to regulation of private health service providers is challenged and found invalid, in the case of inconsistency, the *Privacy Amendment (Private Sector) Act* 2000 (Cth) will take precedence over State legislation on privacy health provisions for the private sector'. Personal Communication from Dr. Danuta Mendelson, Senior Lecturer, School of Law, Deakin University, a medical law specialist, 26 June 2001.

[47] Whether *any* personal information held by an organisation that provides health services should also be regulated by the Act was aired in the Exposure Draft. This raises the problem of separating health personal information from other personal information, and separating health information (i.e. content) from its recordkeeping functional context (health service).

[48] Another approach is found in the PROV/Human Services PROS 99/04 *General Disposal Schedule for Public Health Services Patient Information Records* on retention periods for patient histories, albeit appropriate for stand-alone and single-institutional systems.