Regulating Net Transactions: The Legal Implications for Recordkeeping in Australia

Livia Iacovino

An abridged version of this paper was presented at *Place, Interface and Cyberspace: Archives at the Edge*, the 1998 Annual Conference of the Australian Society of Archivists Inc. Fremantle, Western Australia, August 1998.

ABSTRACT

A broad overview paper on legal issues affecting recordkeeping in cyberspace with particular reference to the applicability of current Australian law on ownership, access and evidence to Net transactions. These legal issues are viewed in terms of the rights and obligations of parties involved in the transactions. It also takes into account the role of 'self-regulation' of industries, individuals and organisations in providing an alternative to greater regulation in cyberspace. This paper argues that the most likely outcome for regulating Net transactions will be a combination of self-regulation and traditional legal sanctions which take into account international, national, and industry controls and standards.

Introduction

There are a range of legal issues that arise in cyberspace. In this paper I will be addressing some of the legal issues that are relevant to recordkeeping as the Internet increasingly becomes a tool for business and social activity. The implications of the use of the Internet for recordkeeping purposes in relation to concepts of ownership, access, and evidence are some of the issues that are particularly relevant to archivists and records managers, and are the main focus of this paper.

The Nature of the Internet

The 'Internet' or the 'Net' is technology most of us are familiar with; the world of networks and connections accessible via the computer. Many organisations, from voluntary to special interest groups, corporate bodies, universities, government and all sorts of individuals, have web sites or home pages. These web sites are the public face of a technology, which together with other mass media such as television, can provide us with contemporaneous participation in events; think of the death of Diana, Princess of Wales or the Australian Constitutional Convention.

The Internet has created the sense of a village community within a global structure. It cuts across national, geographic, cultural, class and legal boundaries. However these legal and cultural boundaries continue to operate and how much they are broken down by the global nature of the Net itself is difficult to predict. In another sense we could say that cyberspace creates its own boundary and a new set of rules to play by.

For those of you who have had the pleasure of seeing Peter Whelan's play *The Herbal Bed* may recall the effects of slander on the reputation of a married woman and on her husband's medical practice in Elizabethan England. The speed with which the defamatory statements took effect in a tightly knit community, with a particular set of values, has some interesting parallels with the impact of such statements in the global village. In cyberspace the extent of the impact of defamatory statements on an individual's reputation is potentially global, and therefore more damaging than ever before. Reversing the effects of unproven allegations when literally exposed to the whole world is almost impossible. I think that gives you an idea of the impact of the Net and the difficulties of applying legal concepts and laws to an apparently borderless world. (Defamation is also an example of regulation in Australia which is inconsistent at the State/territory level, let alone at the national or global level)

The Net as 'community'

Mark Ackerman in 'Metaphors along the Information Superhighway', examines how the new societal metaphors such as 'virtual community', 'collective memory', and 'information superhighway', shape our understanding of the Internet. Ackerman believes that without a proper examination of what these metaphors mean they may in fact be misleading because they distort the reality of what the technologies can achieve. [1] On the other hand it can also

be argued that metaphors provide useful constructs in periods of major paradigm shifts such as that in which we currently live.

'Cyberspace' is often used interchangeably with the term 'Internet'. In fact cyberspace is more than the technology of the Net; it is also a metaphor or construct of being in a 'virtual' rather than a 'physical' community. [2] The term 'community' as a construct for cyberspace is an apt one because it reflects a social rather than a legal entity. This view is central to the argument that the Internet community and its stakeholders can regulate themselves; that they operate under a universal social code.

In cyberspace we operate both as universal man and community member carrying with us our cultural baggage and our own set of personal values. It can therefore be argued that the legal and social relationships engendered by Net transactions, places on the participants in those transactions, a range of rights and responsibilities that underpin the regulation of the Net as a community.

Part 1 Regulation of the Net

What is regulation?

Does 'regulation' mean control via legislation or does it mean using other methods of control outside of the codified law? How much is regulating the Net an ethical issue? The role of ethics and codes of conduct are relevant to the 'self-regulation' models for regulating the Internet. [3] It is useful to initially limit our understanding of regulation to the law made by parliament and the courts, and perhaps consider some traditional definitions below:

Law: the body of rules, whether formally enacted or customary, which a state or community recognises as binding on its members or subjects; a system of such rules, often defined by its source eg statute law, customary law. In English law it refers to statute and common law. [4]

Regulation: control by law. It sets limits upon the manner in which a particular activity may be lawfully undertaken. Certain acts and procedures may be prescribed; others may be prohibited. Usually there is a penalty for a breach. There is an assumption that the law is enforceable. It may also be defined to include social controls or normative systems other than the law proper.

Are Net transactions unregulated?

We can look at the 'big picture' of Net regulation as a global system or move straight down to the transaction or system level and delineate boundaries of regulation. In this paper although I am concentrating on Australia as a boundary, the international nature of the Net makes it necessary to keep the 'big picture' in mind. I will start with the 'big picture'.

Without undertaking a technical expose of the operation of the Net it is important to remember that it is a decentralised system of many networks. The open standard internet protocols were adopted freely. It was the design itself that allowed for its openness. [5]

Many users of the Net argue against its 'regulation'. One of the reasons for this outlook is that the Net is viewed as a tool for improving equality and human and political rights. [6] The Open Internet Policy Principles of the Parliamentary Human Rights Foundation (PHRF) promote the use of the Net as a means of supporting political freedom but also recognise the continued existence of national legal systems that are cognizant of international conventions.

> 'The Internet does not exist in a legal vacuum. For the most part, existing laws can and should regulate conduct on the Internet to the same degree as other forms of conduct. Such laws may differ from country to country, but should conform with the applicable binding human rights obligations contained in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the European Convention on Human Rights.'[7]

There is a popular belief that the NET is UNCONTROLLED in terms of both domestic law and international conventions. It is a result of the confusion between the apparent lack of enforcement of laws on the Net with a conviction that there is an absence of law. I am still amazed to hear people who should know better state that many existing Australian laws do not apply on the Net; copyright is a classic example. Local laws of each jurisdiction *do* apply to activities conducted on the Internet, regardless of enforcement issues. Enforcement and jurisdictional competences in the Internet environment will need to be resolved.

Boundaries have become blurred on the Internet and yet the law is all about boundaries. The Internet may develop its own boundary or it may work through domestic laws which conform to international laws, conventions and treaties. This latter type of international model already exists for intellectual property and commercial law (see Part 2 Recordkeeping in Cyberspace).

Players involved in Net regulation

International bodies

No one is regarded as the 'owner' of the Internet, however the management of domain names and a number of other areas have originated in the United States (US). Some of the Net sites are sponsored by government bodies, and many services are now run commercially. The US is reluctant to let go despite its 'declared' e-commerce strategy which consists of five principles:

- Private sector leadership
- Market-driven medium
- Minimalist government intervention
- Decentralised nature
- Global nature[8]

The OECD and a number of other international bodies have provided voluntary principles on Internet regulation. Internationally there are a number of relevant OECD documents on legal issues. [9]

National governments – Australia

Australian government reports have proposed a number of possible approaches to regulation of the information infrastructure (also known as the `information superhighway') in recent years. [10] The federal current government has established the Information Policy Advisory Council (IPAC) to advise government on a range of online issues and the Electronic Commerce Expert Group has been asked to report on legislation to support electronic commerce (discussed below).

Approaches to regulation of the Net in Australia

A self-regulation model

Self-regulation of the Net may refer to a number of areas. These include the service providers, the users or the technical infrastructure. Regulation may relate to the content on the Net or the rights and obligations in business transactions. On the Internet self-regulation has a strong standing with codes providing an alternative to greater regulation in an environment which is no longer confined to one jurisdiction.

Australian Broadcasting Authority Model

In the 'Investigation into the Content of Online Services Report' by the Australian Broadcasting Authority (ABA) in 1996 the issue of using traditional models for regulation of the media was questioned. [11] The investigation found that the majority of online services are not accommodated by the broadcasting services legislation. The report also discovered that many of the existing regulatory frameworks, eg the broadcasting, publishing, and commercial models were converging. Other regulatory authorities had undertaken their own investigation of the Internet, and as in the case of the ABA, become aware of the overlaps with other authorities and the need for new paradigms, eg the overlap between censorship and invasion of privacy.

The ABA proposed codes of practice, developed within a self-regulatory framework, that would facilitate the productive use of online services in Australia. It recommended industry codes of practice for online service providers. The codes were to be registered with the ABA and within some of the States and Territory censorship laws these codes could be accepted as a defence if legal proceedings were initiated against an industry member. In this sense they have semi-legal force.

Although an Australian 'self-regulation' model has been proposed for the Internet in the ABA model with industry codes of practice for online service providers, the electronic commerce and encryption models indicate more controls, at both the national and international levels. Where other industry and professional codes fit into the picture is still unclear.

Regulatory models – the electronic commerce model

The Australian Electronic Commerce model which has been proposed in a recent report of the Attorney-General's Electronic Commerce Expert Group suggests an overarching legal framework in the form of a Commonwealth law based on the United Nations Commission on International Trade Law (UNICTRAL) Model Law on Electronic Commerce that provides sufficient legal certainty to undertake electronic activities but is not so specific as to tie it to particular technologies or business models. It also aims to ensure legal equivalence of Internet commerce to paper based requirements so that one approach is not advantaged over the other. By adopting an international model it hopes to facilitate the application of international law and conventions. This is in line with the European Community approach while the US is still only looking to uniformity at US federal level. It should be noted that an earlier Australian government report *The Global Information Economy: The Way Ahead*, July 1997, advised on a non-regulatory, market-oriented approach which suggested clarifying existing legislation rather than introducing an overarching piece of legislation. [12]

The definition of electronic commerce adopted by the Expert Group in an earlier statement would cover most recordkeeping on the Net, although it modifies the definition for the commercial setting. It defines electronic commerce as:

> 'In the broadest sense, "electronic commerce" can be used to refer to any information exchange which occurs over the superhighway (ie. by wire or over-the-air transmission or a combination of the two) and encompasses not only commercial transactions, but also *all forms of social intercourse that may take place via the medium of the superhighway; that is, "commerce" in its broadest sense*. (italics added)
>
> In a strictly commercial setting, it would encompass all the steps involved in negotiating, confirming and performing commercial transactions electronically and include both the contractual relationships formed in those transactions and the regulatory or administrative steps necessary to the conduct of those transactions.' [13]

Electronic commerce has raised legal issues that are central to recordkeeping and include: admissibility of electronic evidence; authentication and integrity of electronic communications; time and place of receipt and dispatch of electronic communications, especially as they are relevant to contract formation; acknowledgment of receipt; record retention and management. [14]

The new report identified the following legal issues:

- Need to satisfy both civil and common law systems
- Legal recognition of data messages as related to the performance of obligations
- Requirements of 'writing', 'signature' and 'original' in existing law
- Lack of uniformity in relation to the evidential weight of electronic records
- Retention of electronic records in electronic form not possible under existing legislation
- Clarification of contract formation
- Attribution of data messages

Secure authentication of message sender and the message content were central but the report opposed the specification of technology to be adopted. The report rejects many of the US electronic commerce technology-specific digital signature acts.

Recommendations of coverage in the proposed Commonwealth legislation:

- Scope of Act. Exceptions to law by transaction types, and where the physical record is the right itself (eg titles etc). Transaction is not defined in the report beyond linking the definition to the nature of the transaction, ie commercial or governmental (Note: there is no reference to recordkeeping definitions nor to the 'business records' definitions in evidence acts)
- A basic recognition that information, records and signatures in electronic form should not be denied legal effect on the basis of their electronic form
- A data message should be 'accessible so as to be useable for subsequent reference' to replace 'in writing' requirements in acts
- Functional equivalence of electronic signatures
- Reliability of author identity and content approval to be as reliable as possible at the time the method was

used
- Complete and unaltered information as equivalent to originality
- Commonwealth and NSW evidence model to be adopted to satisfy requirements for admissibility of electronic documents
- An electronic equivalence for the retention of electronic and paper-based retention requirements (Note: It does not go as far as the Massachusetts Electronic Records and Signature Act 1997 (Draft Bill) which requires accurate reproduction of the original record as it existed at the time in question and retention for as long as required by law)
- Validity of data messages in contract formation
- Onus on addressee to prove that a message was sent by the originator or with their authority as in the paper world (in common law), ie the addressee needs to authenticate the originator's identity
- Time and place of despatch rules; time zone differences covered [15]

Electronic commerce is highlighting recordkeeping issues, and associated legal uncertainties. However from the report it appears to have a narrow view of a business transaction, and fails to link individual transactions including email to a business activity. The advantage of the electronic commerce model is that works within an international model which has a proven track record for enforcing contracts in different jurisdictions.

Part 2 Recordkeeping in Cyberspace

Having considered the models for regulation of the Net that have been proposed in Australia I would now like to turn to some of the legal issues that are particularly relevant to recordkeeping in cyberspace.

In cyberspace information appears as a 'seamless web of information', where we can move from site to site, from marketing-type information to records of business processes. The user or client is not aware of the differences. This is radically different from the past when access to records was from defined physical places.

As we move into what may be considered the third generation of the Net away from its first cosy use by academics with their own codes of behaviour, to the second wave of the 'free for all', to the current use of the Net by government and business to undertake day to day business activity, and as a means of disseminating all kinds of information, the recordkeeping and regulatory implications are taking a predominant role.

Transacting business on the Net has been a slower phenomenon in Australia than in the US. This partly attributable to the perceived lack of reliability of the Internet for business transactions. However more and more organisations are beginning to use the Net technology not just as a means to advertise their services, but also to undertake normal business activities. Businesses are setting up 'intranets', and 'extranets' and thus demarcating the use of the Net for specific business functions.

Regulation and recordkeeping

Although records as evidence of business and social activity are only a fraction of Net activity, and from the outsiders perspective they will appear the same as any other data accessed from a web site, their regulatory requirements will differ from other forms of recorded information. [16]

For recordkeepers and the recordkeeping professions maintaining the integrity of records over time is one of the most important legal issues in cyberspace. We will need to ask:

- How can we reconstruct actions on the Net?
- Who owns the records and has control over them?
- Who can have access to the records and under what conditions?
- Do the records provide evidence of a contractual or other legal relationship?

We need to place these questions into the context of recordkeeping activities. Two definitions that capture the nature of **recordkeeping** are:

Recordkeeping: `is making and maintaining *complete, accurate and reliable evidence of business transactions* in the form of records'. [17] It is an activity that aims to generate, control and maintain a *reliable record of actions* of a physical or organisational body. [18]

Recordkeeping activities are themselves regulated by legislative and other controls to ensure that reliable records are captured, maintained and made accessible over time. This will depend on the regulatory environment in which a recordkeeping system lives and the employment of appropriate technology. As Barbara Reed has stated

recordkeeping is a contingent activity. [19] How reliable we want a record to be will depend on the nature of the activity undertaken.

Jurisdictional context
The regulation of recordkeeping practices of organisations has depended on the laws relevant to persons (physical or legal) within the jurisdiction in which they operate, and has been largely determined by laws which:

- Prescribe which records need to be retained beyond their business use, (these laws may not actually specify the creation or retention of 'records' but in order to comply with the law there needs to be evidence that a legal requirement was met, eg product liability laws require evidence of the process of manufacture of a product)
- Provide access to records over time to those outside the organisation that created the records
- Define the ownership and custody over records
- Ensure their integrity (reliability and authenticity) is maintained as evidence
- Regulate recordkeeping standards eg via archival legislation

Do these issues change in the Internet environment? Relevant issues include:

- Is the concept of a national jurisdiction meaningless?
- Is the organisational perspective of 'regulation' pertaining to a specific industry as well as laws that are relevant to recordkeeping in general, often in procedural law, rather than substantive law, still relevant?
- How has the development of 'small government' and the globalisation of the economy changed the business and legal environment?

These questions are beyond the immediate scope of this paper but are larger issues that need to be kept in mind when we look at recordkeeping issues in the Internet environment.

Legal issues surrounding evidence, ownership and access to Net transactions

What are the implications of the use of the Internet for recordkeeping purposes in relation to existing concepts of ownership, access and evidence? Is the current Australian legal system equipped to control the ownership, access and evidential aspects of recordkeeping in cyberspace? In the Internet environment maintaining the integrity of transactions of business and social activity, and ensuring protection of information in them from inappropriate disclosure may be difficult to enforce under existing legislation. Other regulatory sources or models may be more appropriate.

An important issue to bear in mind is that in Australia the power to legislate on particular matters is divided between the Commonwealth and the States and has placed a number of obstacles in the way of a uniform approach to a range of areas of law-making, eg defamation, censorship, privacy, and evidence. This fragmentation within Australia makes an international consensus even more difficult in areas that require regulation of recordkeeping activities on the Net. The attempts to make evidence law uniform throughout Australia is one example.

There is obviously a range of substantive law with which organisations and individuals must comply whether transacting via the Net or via other modes of communication. These include consumer protection, taxation and contract law. Some of these areas of law already provide a strong incentive for reliable recordkeeping.

Business transactions on the Net as evidence

The word 'evidence' is used here in both in its recordkeeping and legal usages, that is records as evidence of business and social activity and as judicial evidence.

The evidential issues relevant to electronic transactions on the Net are often submerged under discussions on security and encryption. The contractual nature of many business transactions necessitates that their evidential qualities be present. Secure systems adopting encryption technologies are central to the success of the Internet for recordkeeping. National governments including Australia and the US, as well as international governments and organisations are all developing technologies for this purpose, not often without controversy. In addition to cryptography's importance for authentication, there are other benefits which include protection of privacy and confidentiality, depending on how surveillance and law enforcement agencies are prevented from misusing encryption technologies for surveillance.

We need to ensure that recordkeeping evidential requirements are extended to Net transactions by being built into the systems adopted. The recordkeeping questions are:

- Are we revisiting the problems of electronic information systems without recordkeeping functionality in the Internet environment?
- Can intranet systems linked to the Net retrieve transactions with all their contextual attributes?
- Are government studies addressing the issue of retaining records as records over any length of time on the Net?
- Can records be recreated when the system and data is migrated?

Recent Australian government reports on electronic commerce do not address these issues fully. Legislation certainly supports the need to be able to recreate records, not just data. For example in relation to section 262A of *Taxation Act 1936*, Draft Taxation Ruling 97/D4 covers computerised recordkeeping system controls and specifies that data collected and how it has been used must be able to be recreated.

Recognition of the need to maintain evidence, including the completeness of data that forms part of an Internet transaction for potential legal proceedings, has been recognised internationally by the OECD, and is provided for in their *Guidelines for the Security of Information Systems*, including provision for the diverse rules of admissibility in legal systems of different countries. [20]

Although EDI (electronic document interchange) has provided standards for legally acceptable contractual relations for many years, and has already addressed the issues of secure communications transmitted electronically, it uses a highly structured form of messaging, which does not resemble email and other software currently used for Net transactions. Contracting over the Internet involves free form of communication, thus EDI principles are not applicable. Contractual issues reinforce the need for reliable evidence. [21]

Australian laws of evidence and Net transactions
Current legislative framework

The laws of evidence are relevant to the admissibility of documents and records as evidence by the courts, ie they are the rules which determine what and how records may be introduced into judicial proceedings.

The admissibility of Net transactions would appear to be covered by the provisions of the 1995 Commonwealth and NSW Evidence Acts, and the business and computer records provisions of other Australian jurisdictions. [22] This is also the view expressed in the Attorney-General's Electronic Commerce Expert Group report. Two features in the 1995 Evidence Acts which are particularly relevant to transactions on the Net as judicial evidence are:

- Abolition of the original document rule, replacing it with simple means of giving evidence of the contents of documents, including documents held in computer and other non-paper forms
- Provisions for easier proof of, and presumptions about, business and official records, and the use of email, fax and other means of communication

Another important section of the *Evidence Act 1995* (Cth) is Part 4.3, 'Facilitation of proof". S 146 deals with *presumptions* about the proper functioning of devices and processes used to produce documents which is not limited to business records, and s 147 which covers *presumptions* about the proper functioning of devices and processes used to produce business records. These presumptions may be challenged but they open the way for the admissibility of Net transactions.

Email as evidence on the Net

Email is one of the most commonly used methods of communication on the Net for business activity. If an email message is a document that forms part of the normal course of business it is as likely to be admitted (or statements/representations from it) as evidence as any other document in any format. Certainly email is subject to Australian FOI laws.

Many organisations do not think of email as a record. In one sense this is true. It may not have the characteristics of a record in that it is not linked to an action, and it is not part of a recordkeeping system. Whether or not it is a 'record' it is discoverable by the courts.

There is insufficient case law for us to know how the courts will deal with records as judicial evidence from the Net. One could presume that it will follow the same principles as the courts have applied to computer and business records in general. It is most likely that reliable records will be of increasing relevance in the Internet environment.

International framework

What about recordkeeping activities of Australian organisations operating overseas when they transact on the Net? Do they have to comply with the evidence laws of those countries? The answer is that they would be subject to the laws of that country, including their evidence laws.

Ownership and access in Net transactions
Current legislative framework

We need some understanding of the legal framework of property law and access rights of non-property holders to ascertain the rights/entitlements and liabilities of the actors involved in a transaction on the Net. There are a range of laws that relate to ownership and control over data and records and the rights of non-owners to gain access to and in some cases amend information in records in the paper world. In terms of the Internet environment our laws in these areas have many deficiencies which are still in the process of being researched and addressed.

The transmission of data and records in electronic form has obscured the distinctions between types of ownership in records. The `form' of a record (form of expression of an original idea as protected by copyright law, eg a play, a film or a literary work), the 'idea' expressed in it (traditionally not protectable by copyright, only in patents if part of a process) and 'access' rights to a record are merging as a direct consequence of the use of electronic means of capturing and transmitting data.

The `form' (eg a web page) can be altered by software, the means of communication are wide-ranging and the concept of `publishing' is no longer the province of publishing houses but that of public networks. At the same time there are emerging claims of a type of `ownership' of data in records by the data subject as distinct from ownership of the tangible record. This latter issue is related to the attempt to control information about oneself, and is linked to the concept of personal privacy.

Personal property law

The simple question as to who owns a record rarely elicits a simple answer. When records were kept in a physical tangible medium they could be defined as chattels, and be bought and sold as personal property. Possession meant prima facie ownership of the thing possessed which could be challenged but was still a powerful weapon. The recognition by the common law that unbroken custody maintained the authenticity of records, meant that public records, in most circumstances, would be admissible in court proceedings.

Can existing personal property law be applied and enforced on the Net? An alternative concept associated with `custody' of records, ie maintaining their integrity without physical possession could encompass specific rights over records by a third party, the records however remaining in the physical possession of the creator. This is recognised in Freedom of Information laws when the government outsources particular activities; the records are considered to be in the possession of the government agency, even if physically with the outsourcer. It is termed as `constructive possession'. [23] A contract could also assign ownership rights and clarify ownership in relation to outsourced recordkeeping functions.

Another approach is to redefine the application of personal property law in relation to ownership of records by applying the law of obligations, so that instead of a relationship between a person and an object (the record) that exists in personal property law, we consider the relationship between two persons and the duties and the rights of those persons in relation to the record. The records also provide a means of protecting the interests of parties involved in a legal relationship. This is a complex concept that has not been applied to recordkeeping and requires further research. This model has merit in the Internet world where legal and social relationships are being re-defined. [24] (See Part 3 The Legal Relationship Model)

Lastly we can abandon principles of property law in relation to ownership of data and records as inappropriate in the electronic world. Property concepts can be replaced by provenance definitions for establishing ownership over records. The Australian Law Reform Commission's *Draft Recommendations Paper 4, Review of the Archives Act 1983*, opts for a provenance approach in lieu of a property approach to ownership of records, which links ownership to the organisation undertaking a government activity; that is records created or received by a government agency in the conduct of its affairs. [25]

Intellectual property law

Intellectual property law with its emphasis on protecting ideas may provide a preferable legal means of control over the ownership of electronic records than concepts of personal property already discussed. However there a number of difficulties here also. Copyright for example protects the form of expression, not the content or ideas or the data in the work. The 'rights' rather than the property are 'intangible' and the item protected needs to have a 'material form', a film, a literary work etc. Edward A. Cavazos and Gavino Morin, in *Cyberspace and the Law*, state that almost everything communicated on the Net is subject to copyright protection, that is as 'an expression that has been fixed in a tangible medium as defined by copyright law'. [26] This would include email or any other communication or transactions on the Net. So there is no question that copyright does subsist in transactions on the Net .

Copyright law is relevant to recordkeeping in terms of:

- establishing ownership, including transfer of ownership of copyright (eg for re-sale)
- providing access to records protected by copyright
- protecting the content in its material form

The importance of intellectual property and proprietary rights varies from context to context, and from the perspective of the owner and the user. One area that is starting to be discussed is the financial value of records and various means of making the information in records, coupled with distilling knowledge from them, a valuable asset for planning and resale. Knowledge discovery coupled with data mining techniques often linking personal information to profile types is an area of convergence with the re-use of data from records.

Copyright/access nexus and recordkeeping on the Net

When records were physically transferred to archival repositories, archivists dealt with copyright issues as separate from access policy. It was uncommon for copyright to be assigned to the archival institution with the actual transfer of the records. Australian copyright law defined records as 'unpublished literary works', with copyright held to be perpetual while the work remained unpublished with some allowance for making a copy of an unpublished work where the author had been dead for more than 50 years and it was more than 75 years since the creation of the work. The idea that archives, as unpublished 'literary works', remained in copyright in perpetuity unless published, was the result of applying a publishing paradigm to records and the association of archival institutions with libraries. The publishing model still holds sway in terms of proposed changes to copyright law.

Expiration of copyright is important in relation to records held over long periods of time particularly if they are digitised and made available via the Internet. With Internet access, records, like other information resources, are likely to be accessible directly from the creating agencies by remote users. 'Transmission', 'copying', and 'reproduction' occur simultaneously, that is as one activity when online public access is available. This means that access to records that may have been free in the paper world when access and copying were separate activities, may have to be paid for as part of copyright permissions. In Canada and the United States the archival communities have been busy making submissions on proposed changes to their copyright acts which they see as providing less rights to users of digitally available records than those in paper form. [27]

Australian developments
The Australian *The Copyright Act 1968* (Cth) has been reviewed in relation to computer software, computerised databases and works generated by or with the assistance of computers, and material being transmitted electronically. Other proposed changes have been the inclusion of statutory moral rights, amendments to the fair dealing provisions, and the introduction of a new transmission right. However very little substantial change to the legislation has taken place.

Australian proposals have been overtaken by international standards set out in the World Intellectual Property Organisation (WIPO) treaties. These treaties are the basis of the *Copyright Reform and the Digital Agenda Discussion Paper*, July 1997. The paper addresses the gaps in protection afforded to copyright resulting from the use of new technologies, in the context of the WIPO Copyright Treaty and the Performances and Phonograms Treaty 1996. A number of new rights and enforcement measures have been included. The most relevant changes in relation to placing material on the Net relate to a new right, in addition to the transmission right, referred to as the *making available to the public right* which specifically covers uses of copyright in interactive on-demand online services. It could be either separate from or be part of the reproduction right. Australian proposals exclude a situation where simply looking at something on the Net would infringe a reproduction right. [28]

Infringement and enforcement
Generally copyright issues centre on infringement due to unauthorised transmission or downloading of protected data. One must first establish that there is a copyright `work' involved and that it has been infringed. Copyright law has always recognised 'authorised infringement', that is a party authorising the act that infringes copyright is liable even if they do not carry out the act themselves. Shared liability between the user and the information provider for breaches of copyright continues to apply on the Net. In fact the liability of the provider increases with involvement in content selection. [29] Technological approaches to copyright protection, eg security, encryption are also relevant to enforcement.

International framework

Intellectual property has an existing international framework and a forum which provides protection outside the country of creation of a 'work' at least for the signatories of the Berne Convention. The international treaties only cover minimum standards, but domestic copyright law differs substantially from country to country. In relation to researching this paper I found many differences between European copyright laws, US and Australia. [30]

The disagreements among the Berne convention countries over the 1996 World Intellectual Property Organisation (WIPO) Treaty on Intellectual Property in respect of Databases is a recent example of the difficulties of international agreement on intellectual property. [31] One of the controversial issues here was the new *sui generis* right for databases as a whole to be a separate category, apart from protection for individual content such as an image, which would prevent the use of a substantial part of the database for 15 years, renewable when significantly updated. In theory a database would be protected forever. [32] Compilations of data presently receive protection under copyright in the selection and arrangement of data. The data itself is not protected. The 1992 European Commission Directive on Database Protection is gradually being adopted in European Community (EC) countries. If accepted in the US and Australia it would overturn the 1991 US Supreme Court decision in *Feist Publications, Inc. v. Rural Telephone Service*, in which the Court rejected a claim of copyright for data from a telephone directory's white pages, saying that facts cannot be copyrighted, and that lists of names, addresses, and telephone numbers in alphabetical order, are not sufficiently creative to qualify for copyright protection. [33]

The protection of data itself as a form of intellectual property would be the single most important change to copyright law. It appears to be an over reaction to protecting commercial interests on the Web. Will electronic recordkeeping systems be defined as databases for the purposes of copyright law? Although there does not appear to be any real discussion of this possibility the extension of copyright to cover data would have some effect on ownership of the content in records.

Australian and international reforms indicate a continuing protection of material in non-interactive form, with new rights introduced to cover transmission of material over the Net. Increased protection has continued to favour copyright owners at the expense of users.

Access/privacy/ownership nexus in Net transactions

Access as *the regulation or control* of who gets to see specific information and of what use they make of it has specific requirements in Net transactions. A privacy regime *restricts* the use of information about people. Access regimes give data subjects and users *rights* to obtain and use information. This can be done via legislation or self-regulation schemes.

Record creators and keepers have obligations to protect information about individuals in records under statute and common law, which may be distinct from proprietary rights. As we have already noted protecting intellectual property in cyberspace can conflict with access and privacy rights and a proper balance needs to be struck between these competing rights. For example ISP's and content providers have to be aware of any infringing copies and show that they have taken reasonable steps to stop these copies being transmitted. They have to compromise the privacy of their clients in order to comply with this aspect of copyright.

The loss of privacy in Net transactions has been singled out as one of the major reasons that individuals and companies have been reluctant to use the Net for business activity. Ensuring privacy in the development of the Internet is a key consideration both in Australia and internationally. The OECD Policy Briefs on *Electronic Commerce* state that:

> 'As electronic commerce develops, the volume and nature of personal data (name, address, interests, purchases...) disclosed on networks during electronic activities and transactions will increase. New

> methods for processing the vast accumulation of data_ such as data mining techniques_ allow the creation of customer profiles that combine demographic data, credit information, usage patterns and details of transactions. If consumers do not have control over the collection and use of their personal data, electronic commerce will facilitate the invasion of their privacy.
>
> But, if consumers are in a position either to decline or to give informed consent to the collection and use of their personal data, electronic commerce will not be different from traditional commerce. In today's world, consumers may participate in fidelity or loyalty shopping plans and choose to exchange their privacy for something they value (lower prices, convenience, personalisation). Businesses and consumers will have to help adjudicate the trade-off between protecting privacy and obtaining the benefits of electronic commerce that they both value. Education on this issue is therefore of primary importance'. [34]

Current legislative framework
Access

Statutory schemes within government for giving access began with access arrangements for older records in the Archives Acts. This has found expression in the thirty year rule. The passing of the Cth *Freedom if Information Act* 1982 brought a fundamental change in the law in Australia relating to access to government held information. Access before had been a *privilege*, now it was a *statutory right*.

Governments around the world have improved public access to government information via the Net, ie information locater systems which direct users to sources of relevant government information. From the users' perspective all government information whether a record or not will be available through a common user interface.

David Roberts in *Documenting the Future*, describes future networked access to documents themselves. [35]

- Users login as `guest users' with access rights and restrictions
- Data will be secured with `firewalls' to separate them from publicly accessible parts
- Applicants use the retrieval tools of the agency's recordkeeping system with necessary security safeguards, therefore reducing time and cost for the agency

This assumes that governments will release records, provide safeguards, and secure the records as time bound into the future and make decisions on archival requirements. Electronic access to government data, both information and records, will involve some continuum in access, and some consideration of bringing the *access provisions* of all legislation dealing with it together, ie the public right to know as expressed in FOI and the right to privacy in privacy legislation.

Which government records *are* made available will depend more on political will rather than the technology of the Net. This is clearly visible in the watering down of FOI legislation both federally and in the states, and the privatisation of government activities which has restricted the ambit of FOI.

Privacy

In Australia both FOI as well as Privacy legislation have been relevant to understanding the statutory rights of access and protection of personal privacy in government records and some private sector records. FOI has provided a means of appealing against government decisions BUT it did not cover what government or third parties did with personal information hence the need for the separate *Privacy Act 1988*. FOI and Privacy have been restricted to the public sector except in relation to the handling of Tax file numbers (and to some government contractors) and credit reporting agencies; some business/industry codes have adopted the Information Privacy Principles (IPP's).

The current federal government has aborted earlier government reports recommending the extension of Privacy legislation to the private sector nationally, with codes of practice for network providers, and quality control exercised by the Privacy Commissioner. [36] Instead the government has opted for voluntary self-regulation, arguing that this would avoid the cost of compliance for businesses. [37] The proposed `National Scheme for Fair Information Practices in the Private Sector', August 1997 does however have a more rigorous standard which will follow `international best practice in fair information practices'. [38] It will be compatible with the existing Commonwealth Privacy laws and be a national scheme for the private sector. It has been an important business risk issue in that Australia's current privacy laws do not conform 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.

Privacy controls have stalled once again on both the Commonwealth and state levels. However it will have to be resolved if e-commerce is to become a reality. Without the extension of privacy legislation to the private sector, and the lack of conformity to 1995 European Directive on Privacy, Net transactions in Australia will not have statutory protection for personal privacy outside of the federal government jurisdiction.

Enforcement of privacy and access in Net transactions

Policy
The management of access on the Net, and privacy in particular, involves control over to whom information is released, and how it is construed or to what use it is put, and how long it is retained. Policy decisions should precede technological solutions.

System design
A recordkeeping system which is designed to be secure, time bound and linked to an access policy should provide adequate privacy protection for the data subject, while ensuring that any rights of the data subject are protected without the need to delete the personal information once it has served its purpose. [39]

Confidential information needs to maintain its quality of confidence to be protected legally. Transmitting confidential information on the Net requires a clear notice that it is confidential as well as appropriate security controls, eg encryption.

Legislation There are limitations in the current privacy principles in our legislation which are based on an `an individual whose identity is apparent' (*Privacy Act 1988* s 6) when identity is not apparent but may reside in the log of web access held on a server. [40]

User/provider agreement
In the United States negotiated privacy between user and provider is available by paying a higher price for greater privacy. User privacy in these agreements between the user and the provider arrange that the provider will only review messages if there is some suspicion of illegality. [41]

Technical solutions
Security/system controls or `privacy technology', for example cryptography appear to provide privacy without recourse to the legal system. Authentication and cryptographic techniques, and electronic signatures ensure security from unauthorised access, but rely on an organisation or person who can be trusted with the keys to the encryption regime. If public keys are made available to law enforcement agencies via the *Telecommunications (Interception Act) 1901* pursuant to a warrant allowing it access to the key, privacy will be compromised. [42]

Other security approaches include an identity card based on DNA characteristics to access systems; or software that identifies mouse pointing patterns. Web browsers and sites can evolve architectures that identify individuals for specific purposes only.

International framework

The *Privacy Act 1988* is based in OECD principles, and so like intellectual property has an international context that is important in terms of Internet developments. The extension of Australian privacy law to the private sector, would bring Australia in line with international approaches. Current domestic information superhighways with there own privacy regulations need to evolve in the global information infrastructure. Australia needs to continue to participate in the OECD developments. For any mechanism of control on privacy to be effective on the Net the service provider will have to agree to international regulations, not just domestic law.

But whose responsibility is it to protect privacy? Government, market forces, or self-regulation models? We have to think in terms of the relationships between the players, and their respective rights and duties, in the online world. Codes of conduct and other self -regulatory issues have an important part to play in regulating the global Internet community.

Having summarised the legal aspects of evidence, ownership, access and privacy of relevance to recordkeeping on the Net I would like to posit an approach which can be applied to analysing the legal and social responsibilities of players involved in Net transactions.

Part 3 The Legal Relationship Model

As discussed in this paper in regulating Net transactions in Australia, existing legislation is being slowly modified, eg copyright law, or new legislation is being proposed, eg electronic commerce legislation, within international frameworks. These approaches are all dependent on technology that is secure although never likely to be foolproof. In other areas industry and professional codes within a national framework are being proposed to enhance legislative approaches to regulating the Net, eg the ABA model, and the adoption of industry privacy principles by the banking and health sectors. In addition private arrangements via contract law or obligations arising from relationships between parties transacting on the Net are beginning to take on an important role. There are also new ways of interpreting legal principles of ownership and the obligations arising from ownership between the parties involved in a transaction. The concept of a legal relationship is one way of placing on the participants in Net transactions a range of legal and social responsibilities that underpin the regulation of the Net as a community.

What is a legal relationship?

'The notion of a legal relationship is a shorthand way of saying two persons are related by some act, event or dealing'. [43] The common law system recognises a range of legal relationships, such as commercial and professional relationships, the nature of which determine the rights and obligations of the parties concerned. It gives a legal personality to individuals and to organisations (as natural or legal persons) in order to recognise them as holders of rights and obligations and to regulate them, an incorporated company is a good example. Legal relationships imply a duty to another individual or legal entity which in turn creates a right in the other party (eg debtor/creditor relationship; the bank provides a person credit, it has a right to be paid back; the debtor has a duty to pay the money back).

The duties and obligations of parties in legal relationships can apply to their rights of ownership in records as creators or rights of access as data subjects, which in turn are underpinned by records providing proof of the existence of the rights or obligations. It is a model that focuses on the actors involved in the recordkeeping processes and the responsibilities that arise from those processes. The legal relationship model draws from concepts found both in archival science and in jurisprudence.

Applying the legal relationship model to NET transactions

Internet actors/players

We can apply the legal relationship model to Net transactions. The model helps us to identify the obligations of parties involved in the transaction. In regulating transactions on the Net, there are a number of levels and players involved. These include global, national, state, organisational, and the individual players. Where these players fit into the legal relationship model requires further research. Before we can test this relationship model to Internet transactions we need to look at the players on the Net.

The following is a useful breakdown of Net actors:

Network provider: provides the physical connections; links to the infrastructure of the Internet; routers, hosts and pipes, ie the telecommunications, government, and academic networks.
Service provider/access provider (ISP): provides a range of access services on leased lines, including client software; services include dial-up accounts for home use; permanent connections for commercial use; may provide additional services such as Web hosting and design. Originally universities provided it to staff and students; now run by commercial organisations, including telephone companies.
Host: provides the storage space accessible via the Internet; the servers; may be involved with placing material on the host; may run newsgroups; provides domain name server.
Administrators: provide internet protocols and domain names.
Content provider: whoever is placing content on the web; eg companies, individuals; linkages to other sites.
Navigation providers: sift the content using 'search engines', or provide directories.
Transaction facilitators: provide security and identification of the parties in the transaction; they act as trusted intermediaries. See below regarding the 'cybernotary' concept.

From: *Internet Lawand Regulation*, a specially commissioned report, edited by Graham J. H. Smith and

contributors, FT Law and Tax, London, 1996, Chapter 1, 'Overview of the Internet'.

From the recordkeeping view of a legal relationship arising from players in a Net transaction we may recognise familiar actors, as well as new players or old ones in new guises. See figure 1 below. 

Competent author: the person having authority to carry out an act; an entity/corporate body capable of acting legally.
Recipient/Addressee: the person for whom the message is intended.
Third party: `one who is a stranger to a transaction or proceeding' (From *Osborn's Concise Law Dictionary*, 8th edn, eds Leslie Rutherford and Sheila Bone, Sweet and Maxwell, London, 1993).
Data subject: the person who is the subject of, or referenced in a transaction; that is referenced in the content/subject matter of the transaction.
Service provider: the provider of a range of access services, including client software; services include dial-up accounts for home use; permanent connections for commercial use; may provide additional services such as Web hosting and design.
Communications carrier: provider of telecommunications service.
Net regulators: Government authorities; legal and social enforcement mechanisms.

Notes for Figure 1:
Net Players: persons (physical or legal) that form part of the transaction or that have rights or obligations as a consequence of that transaction.

Transaction: an act aiming to change the relationship between two or more parties which is communicated and forms part of an activity and results in a specific legal consequence. In an electronic transaction it must cross electronic boundaries and be captured (made and received) by a system.

Competent author: the legal actor/ `person' having the capacity/authority to act legally in his/her own right. There may be more than one author.

Data subject: may have statutory rights of access or privacy protection

Third party: the third party sits outside the transaction but has rights because of the relationship with the first and second parties to the transaction as a result of the consequences of the transaction. These could be general users, recordkeeping professionals, or transaction facilitators, that is authenticators, such as the 'cybernotary', [44] 'gatekeeper' [45] or archival authorities in their primary role of trusted third parties. The concept of the cybernotary, a trusted third party that provides a guarantee/certificate for each transaction has links to that of a legal notary, one the oldest recordkeepers in society, and also a role archival authorities have played. [46]

The liability of *transaction facilitators* for incorrectly identifying a person is a key issue identified in Australian Electronic Commerce report. [47] The duties and potential liabilities of the accreditation authorities (AC) have not been clarified, ie what is their duty of care when issuing a certificate in terms of verifying the person's credibility?

In figure 1 the use of broken lines denotes a tenuous relationship between the service provider and the actors involved in the transaction. There is insufficient case law on liability of service providers to clearly define their legal obligations to the parties involved in a transaction. [48]

A player on the Internet can have a number of roles. When determining the legal consequences of activities on the Internet, it is important to identify which roles the person is performing, eg a service provider may perform the same roles of the network provider, host and access provider. The fact that a number of the telecommunications carriers eg Telstra also provide internet services exemplifies the complexity of the legal relationship model when an entity has a number of roles (possibly conflicting) and thus legal obligations to several parties.

Different actors in a Net transaction will have different property and access rights. Whether it is the author or the recipient who owns the records, has custody or possession, can provide access to a third party, can retain or destroy records will also depend on how the legal system views ownership rights and other rights (as discussed in Part 2 of this paper).

There is therefore a need to identify the role and legal activity involved. These could include contractual relations:

- The relationship between the web site owner and the host service provider. A typical service contract between a host and an owner will generally ensure that the owner is liable for content placed on the Net
- The relationship between the end user and ISP would include the extent of liability the ISP takes for the end user's transactions on the net

The differences between Net transactions and those in the paper world arise from the fact that there are more actors involved that may interfere in the transaction and this may occur outside of the jurisdiction of the legal system in which transaction occurs. It is too early for us to ascertain how far the actors can be regulated using the laws in Australia and what other rule sets apply to the enforcement of rights and obligations on the Net. [49]

NET as a community and the relationship model

We can also apply the legal relationship model to the Internet as a community in which the reliability of commercial transactions, rely not only on the technological and legal solutions, but also social ones. Michael Froomkin makes it clear that no cryptography or digital signature can guarantee that a transaction is from the person it purports to be or was sent exactly when it is purported to be sent. 'These partly cryptographic, partly social, protocols require new entities, or new relationships with existing entities, but the duties and liabilities of those entities are uncertain. Until these uncertainties are resolved, they risk inhibiting the spread of the most interesting forms of electronic commerce and causing unnecessary litigation'. [50]

The Australian Electronic Commerce Group Report identified the key issues to facilitate e-commerce were a mechanism to reliably prove the origin, receipt and integrity of information, to identify the parties involved in the transactions, to assess any associated risk, and the ability to have legal recourse if something goes wrong, regardless of the geographic location of the parties involved. The Electronic Commerce Report found that commercial relationships have worked in a bounded context, eg within the banking community because of commercial practice. The Report also discovered that the lack of a pre-existing relationship between two parties transacting on the Net prevents electronic commerce developing.

On the Internet how will ongoing rights and responsibilities be maintained beyond individual contractual obligations? The concept of a legal and social relationship can assist by building on trust, both as an ethical and a commercial concept. Trust cannot be provided by a system's security features alone. It is also built on the ability of persons (corporate or physical) to show that they are trustworthy. It is similar to the trust we have in a company that has a long standing good reputation in its business dealings. Re-establishing legal and social relationships are essential to the regulation of Internet transactions.

Conclusion

The combination of self-regulation and traditional legal sanctions are likely to be the most effective approach to regulating recordkeeping activities which are no longer confined to one jurisdiction. Both nationally and internationally, as promoted by the EC and international bodies such as the OECD, the trend is towards increased regulation over Net transactions to provide a secure business environment. Australian laws and codes must change further to accommodate international trends. Recordkeeping will play an increasingly important role in Internet transactions that are linked to business and social activity. The risks of not creating reliable records that may need to be retrievable with all their recordkeeping features over time will continue to be the central issue for recordkeeping regulation.

Metaphors for the Internet as a 'virtual community' with its own rules need to be carefully drawn as they may ignore existing rules which operate as social and legal constructs of behaviour. The relationships of players on the Internet may appear more complex than in the past but establishing the relationships between key parties to a transaction are still fundamental to ascertaining their legal obligations whether in the online or offline world.

1. Mark Ackerman, 'Metaphors along the Information Superhighway' in Proceedings of the Symposium on Directions and Impacts of Advanced Computing (DIAC'94), Cambridge, Mass, April, 1994, http://www.ics.uci.edu/~ackerman/docs/diac94/diac.final.html accessed 17/5/97.
2. It was in fact a term coined from William Gibson's science fiction novel the Neuromancer. 'Cyberspace was a consensual hallucination that felt and looked like a physical space but actually was a computer-generated construct representing abstract data. People could plug into data systems and networks and have the sense they were actually entering a place that had no correlation in physical reality. In this setting, people carried out business transactions, communicated with one another, worked, played, and, as they have done in every other place they had occupied, broke the law'. From Edward A. Cavazos and Gavino Morin, *Cyberspace and the Law*, MIT Press, Cambridge, Mass., London, 1994, p. 1.
3. Peter Leonard, 'Ethics in Cyberspace', *Internet Law Anthology*, ed. Peter Leonard, Prospect Intelligence Report, Prospect

Publishing, Sydney, 1997, pp. 140-141.

4. The Shorter Oxford English Dictionary on Historical Principles, 3rd edn. Oxford University Press, Oxford, 1984, Vol. 1.
5. Sharon Eisner Gillett and Mitchell Kapor, The Self-Governing Internet: Coordination by Design, prepared for Coordination and Administration of the Internet, Workshop, Kennedy School of Government, Harvard University, September 8-10, 1996, http://ccs.mit.edu/CCSWP197.html accessed 23/3/98. Also in Coordination of the Internet, edited by Brian Kahin and James Keller, MIT Press, 1997.
6. In the 'Preamble', of the Open Internet Policy Principles of the Parliamentary Human Rights Foundation the nature of the Net is described in the following terms: 'The Internet is an inherently open, decentralized communications infrastructure which is ideally suited to support the free exchange of ideas, a rich political discourse, and a vibrant economy. The decentralized architecture of the Internet provides an abundance of communication opportunities, and gives users an unprecedented degree of control over the information that they receive. As organizations devoted to basic human rights, the growth of the Internet, and the flourishing of democratic culture, we believe that the foregoing principles will ensure that the Internet remains open and continues to support basic democratic values'.

   From 'Preamble', *PHRF Conference, Brussels, Belgium 23 November 1996*; Open Internet Policy Principles; The Parliamentary Human Rights Foundation (PHRF) is a worldwide, voluntary, non-partisan, not-for-profit organization committed to the promotion of human rights. http://www.cpsr.org/cpsr/lists/rre/Open_Internet_Policy_Principle accessed 1/5/98.

7. Ibid
8. As reported in 'Alston Rethinks US Net plans', *The Age*, 21 April 1998.
9. See the OECD web site at http://www.oecd.org/ In particular see Global Information Infrastructure – Global Information Society (GII-GIS), http://www.oecd.org/dsti/sti/it/ec/prod/gii-gis.htm accessed 25/5/98.

   OECD, Dismantling the Barriers to Global Electronic Commerce, http://www.oecd.org/dsti/sti/it/ec/prod/dismantl.htm Latest update16 October 1997, accessed 25/5/98.

   OECD, Electronic Commerce, Opportunities and Challenges for Government (The "Sacher Report"); http://www.oecd.org/dsti/sti/it/ec/act/sacher.htm Latest update 18 September 1997, accessed 25/5/98.

   OECD Policy Briefs, Electronic Commerce Policy Brief, No1, 1997 http://www.oecd.org/publications/Pol_brief/9701_Pol.htm accessed 25/5/98.

   See also Greg Tucker, `Security, Privacy and Intellectual Property Rights in the Information Infrastructure', in *KISDI-OECD Joint Conference on Information Infrastructure: The Vision for the New World Order, Korea Information Society Development Institute and the Organisation for Economic Co-operation and development*, Seoul, 1995, pp. 150-152.

10. Earlier reports include the National Information Services Council (NISC) Agenda Papers, Canberra, 1995. The Broadband Services Expert Group, Networking Australia's Future: Final Report, Canberra, 1995 (Both papers are on the Australian Government, Government Policy and the Information Superhighway web site, http://www.nla.gov.au/lis/govnii.html).
11. 'There is no central control or ownership of them [the media]and the functions performed by the participants in the online environment are not as fixed as in existing publications and broadcasting models. Significantly, any person can create material and make it available online' From Australian Broadcasting Authority, 'Investigation into the Content of Online Services Report', Executive summary, 30 June 1996, http://www.dca.gov.au/aba/olsexe.htm, accessed 9/10/97.
12. Attorney-General's Electronic Commerce Expert Group, Report of the Electronic Commerce Expert Group to the Attorney General, Electronic Commerce: Building the Legal Framework, 31 March 1998. http://law.gov.au/aghome/advisory/eceg/single.htm accessed 11/5/98.
13. Attorney-General's Electronic Commerce Expert Group, What is Electronic Commerce? http://law.gov.au/aghome/advisory/eceg/eceg.htm accessed 28/1/98.
14. Ibid
15. Report of the Electronic Commerce Expert Group to the Attorney General, op. cit.
    One of the most useful outcomes from the electronic commerce legal analysis is that it forces the legal community to look at terms such as 'signature' in terms of what it performs, and addresses issues that are part of recordkeeping concepts but have been lost in laws that have developed in the paper world. However the report does not address how a transaction relates to an activity. Unfortunately the report has little to say about the Australian Records Management Standard AS 4390, Records Management, and the proposed international Records Management Standard. Archives legislation is defined in its preservation role not in its regulatory role, see 2.10.13 in particular, which states that records retention is imposed by statute law.
16. See for example Government Information Locater Systems such Aus GILS which provide access to government resources via knowledge structures.
17. *Records and Recordkeeping: Introducing New Concepts*, RMO Catalogue # 18, Records Management Office of New South Wales, November 1994 p. 4.
18. Luciana Duranti, `The Recordkeeper in Society, An International Perspective', in *Proceedings of the 14th National Convention of the Records Management Association of Australia, 15-17th September 1997*, Perth, Records Management Association of Australia, 1997, p. 7.
19. Barbara Reed, 'Metadata: Core Record or Core Business?', *Archives and Manuscripts*, Vol. 25, No. 2, Nov. 1997, pp. 221-222.
20. OECD, Guidelines for the Security of Information Systems, 1992, http://www.oecd.org/dsti/sti/it/secur/prod/e_secur.htm accessed 25/5/98.
21. *Internet Law and Regulation*, a specially commissioned report, edited by Graham J. H. Smith and contributors, FT Law and Tax, London, 1996, Chapter 8.
22. The acceptance of documentary evidence in court proceedings in the Australian legal system in which the contents of documents have been regarded as hearsay has evolved gradually. `Business records' provisions are particularly important in the way documentary evidence including computer records have been accepted as judicial evidence. Business records provisions exist in all Australian jurisdictions, and are based on the notion that since businesses must keep reasonably accurate records if they are to stay in business, these records are likely to be sources of sufficiently accurate information to be acceptable as evidence. Business records definition can be used for admitting most documentary evidence because it is broad enough to get

around the problem of changes in the technology used to produce records.

Computer records had been recognised in most Australian jurisdictions either by inserting legislative provisions which are directed to the admissibility of computer evidence or by seeing computer records as one type of business record. The evidence legislation before the 1995 Acts viewed computer generated evidence as copies. The new evidence Acts no longer distinguish between computer-generated or other records. Email and electronic records are potentially admissible subject to existing laws of evidence.

23. Madeleine Campbell, `FOI Access to Electronic Records', in *Playing for Keeps*, ed. Stephen Yorke, Australian Archives, Canberra, 1995, p. 191.
24. *The Law of Commercial and Professional Relationships*,. ed. Simon Fisher, FT Law & Tax, South Melbourne, 1996.
25. Australian Law Reform Commission, Draft Recommendations Paper 4, Review of the Archives Act 1983, Sydney, December 1997.
26. Cavazos and Morin, op. cit., p. 56
27. Council of the Society of American Archivists, 'Basic Principles for Managing Intellectual Property in the Digital Environment: An Archival Perspective', 26 August 1997. http://www.ninch.cni.org/ISSUES/COPYRIGHT/Principles/nha_Complete.html
28. Attorney-General's Department and Department of Communications and the Arts, Copyright Reform and the Digital Agenda Discussion Paper, July 1997 pp. 20-21. http://law.gov/au/publications/digital.htm accessed 28/1/98.
Under the proposed World Intellectual Property Organisation (WIPO) Treaty 1996 'works' made available by transmission are not considered published in the sense of distributed in a tangible form; this is to allow the traditional right of protection to published works such as books to continue as a separate right.
29. Peter Gleeson, 'The Internet, Email and Bulletin Boards: Who's Liable for What?' in *Computers and the Law*, Leo Cussen Institute, May 1996, pp. 1-19.
The US National Information Copyright Infrastructure Protection Bill 1995 included a provision that on-line service providers would be responsible for infringing copyright - this stalled the Act (see http://www.eff.org/pub/Intellectual_property/NIIcopyright_bill).
30. 'Austria Implements Database Directive', in *International Computer Law Observer*, February, 1998, No.3. The International Computer Law Observer (ICLO) is an e-mail report providing monthly coverage of significant legal developments from around the world relating to computers, technology and the Internet. Back issues and a listing of the Editorial Board can be found at http://www.lawcircle.com/observer.
31. World Intellectual Property Organisation Diplomatic Conference,Geneva, December 2 to 20, 1996, Basic Proposal for the Substantive Provisions of the Treaty on Intellectual Property in Respect of Databases to be considered by the Diplomatic Conference,30 August, 1996 http://www.loc.gov/copyright/wipo6.html accessed 1/6/98.
32. *Internet Law and Regulation*, op.cit., p. 22.
33. Charles Oppenheim, *The Legal and Regulatory Environment for Electronic Information*, 2nd. edn, Infonortics Ltd., Calne, 1995, p. 22.
34. OECD, Electronic Commerce Policy Brief, No. 1, 1997, op. cit.
35. *Documenting the Future, Policies and Strategies for Electronic Recordkeeping in the New South Wales Public Sector*, RMO NSW, July 1995.
36. The National Information Services Council (NISC), op. cit., pp. 83-85; and The Broadband Services Expert Group, op. cit., Risks Section 6.
37. The review of the Commonwealth FOI Act in 1995 suggested the extension of the Privacy Act to the private sector. See 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, Canberra: Australian Government Publishing Service, 1995. Since then there have been reports in some states (NSW and VIC) and federally as presented in the AG's Report in Sept. 1996 to the Privacy Commissioner supporting the extention of the existing Commonwealth privacy regime to the private sector. http://www.agps.gov.au/customer/agd/clrc/privacy.htm accessed 3/10/97. In March 1997 the Federal Government decided not to extend the Privacy Act to the private sector at the same time as it outsourced its IT infrastructure. Originally the outsourced IT was meant to be covered by the changes to the Privacy Act.
38. Privacy Commissioner, 'Information Privacy in Australia: National Scheme for Fair Information Practices in the Private Sector' August 1997, http://www2.austlii.edu.au/itlaw/..nal_scheme/national-INFOMAT.html accessed 9/12/97. See also National Principles for the Fair Handling of Personal Information, Federal Privacy Commissioner, February 1998. This document is the first stage in the development of a national privacy scheme for Australia. It should also be noted that in July Victoria issued a Data Protection Bill and an Electronic Commerce Framework Bill. The Privacy Bill provides for a data protection regime for both the public and private sectors in Victoria that allows for integration into a national data protection scheme if one is established. The Electronic Commerce Framework Bill will provide for online signing, such as contracts, and reliable levels of security and authentication to parties involved in electronic commerce. See State of Victoria, Department of State Development, Multimedia Victoria 21, Discussion Paper, Information Privacy in Victoria: Data Protection Bill and Discussion Paper, Promoting Electronic Business: Electronic Commerce Framework Bill, July 1998.
39. This is a current but not a new debate. The Attorney General's Report, Sept. 1996 to the Privacy Commissioner, op. cit., recommended extending the privacy regime to the private sector, and adding the deletion principle to the IPP's. From the recordkeeping angle controls on unauthorised disclosure of private details of identifiable persons must be secured if we are to argue for the continued retention of personal information beyond its immediate use.
40. Graham Greenleaf, `Privacy Principles - Irrelevant to Cyberspace?', in *Internet Law Anthology*, op. cit., pp. 129-138.
41. Lance Rose, *Netlaw: Your Rights in the Online World*, Osborne McGraw-Hill, 1995, pp. 171-185.
42. Natalia Yastreboff, `Encryption and Australian Government Policy', in *Internet Law Anthology*, op. cit., pp. 108- 115.
43. Fisher, op. cit., p. 17.
44. Michael Fromkin, 'The Essential Role of Trusted Third Parties in Electronic Commerce', Version 1.02 Oct. 14, 1996, also in *Oregon Law Review,* No. 49, 1996. http://www.law.miami.edu/~froomkin/articles/trusted.htm accessed 21/1/98.
45. See the role of Gatekeeper: 'The creation of a Government Public Key Authority (GPKA) to manage the Government Public Key Infrastructure (GPKI), and oversight the accreditation of certification authority service providers and public key technology products'.
http://www.ogit.gov.au/gatekeeper/aboutgatekeeper.html accessed 19/5/98. 'GATEKEEPER was developed by the Office of Government Information Technology in response to the identified needs of agencies to introduce public key technology to support authentication and identification in Government online transactions. The strategy ensures that this is done under a whole

of government framework that ensures interoperability, integrity, authenticity and trust for both agencies and their customers.' Could an archival authority play the role of gatekeeper? http://www.ogit.gov.au/gatekeeper/aboutgatekeeper.html accessed 19/5/98.
46. Froomkin, op. cit., p. 7.
47. Report of the Electronic Commerce Expert Group to the Attorney General, op. cit., p. 84.
48. *Internet Law and Regulation*, op. cit., pp. 18-19. The Netcom case.
49. David G. Post, 'Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace', *OnLine*, 1995, article 3, http://www.law.cornell.edu/jol/post.html accessed 24/4/98.
50. Froomkin, op. cit, p. 1.

Back to top