8 LEGAL AND SOCIAL RELATIONSHIPS: AN ALTERNATIVE INTERNET REGULATORY MODEL

Evolving Internet regulatory models have much in common with the 'self-regulation' and ethical controls of communities of common interest, which continue to depend on the identity and trust of recordkeeping participants. Legal and social relationships within communities of common interest provide an alternative regulatory model for recordkeeping regimes, and a viable tool for identifying the rights and obligations of participants, in particular in relation to ownership, access and evidence in Internet 'business' transactions. The legal and social relationship cyberspace model focuses on the rights, obligations and liabilities of Internet legal and social actors in recordkeeping transactions, with reference to professional, governmental and business relationships online.

The Internet's features have presented new challenges to record authenticity in terms of storing and preserving 'the record' that may be on many servers anywhere in the world. International and general standards for recordkeeping are important in the global environment, as they have been developed to be context-neutral.[1]

8.1 Internet as community and the relationship model

The legal and social relationship model can be applied 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 have been sent. Froomkin says:

[1] For example, InterPARES 1 has requirements for preserving authentic electronic records which leave individual countries to contextualise them, and the Monash Recordkeeping Metadata Schema is also organisational-neutral, so it is applicable to any distributed enterprise using Internet technologies.

> 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.[2]

For Francis Fukuyama the Internet in the 1970s and 1980s operated on the basis of a community of shared values, used mainly by the government and the academic community. The 'open' Internet as a community based on reciprocal moral obligation may be difficult to implement without a set of common values by those using it. He views hackers as 'inadequately socialised'.[3] Moves towards building an international consensus on ethical and legal principles applicable in cyberspace have been addressed in a number of domains, for example through UNESCO.[4] The success in transferring shared ethical norms to Internet participants is a critical factor to the success of both electronic business and social communication.

In the online environment elements of trust found in communities and social relationships are difficult to replicate. Can 'virtual communities' substitute for face to face contact? How will ongoing rights and responsibilities be maintained beyond individual contractual obligations? Moral communities take a long time to form and it is not possible to expect the Internet to achieve the same level of trust that has taken thousands of years to build in earlier societies.[5]

The concept of a legal and social relationship can assist by building on trust, both as an ethical and a commercial concept. A system's security features alone cannot provide trust. It is also built on the ability of persons (corporate or physical) to show that they are trustworthy. It is similar to the trust in a company that has a long-standing good reputation in its business dealings. Re-establishing relationships of trust, not only as legal duties but also ethical obligations, are essential to the regulation of Internet transactions.

---

[2] Michael A. Froomkin, 'The Essential Role of Trusted Third Parties in Electronic Commerce', Version 1.02. 14 Oct., 1996, p. 1.

[3] Francis Fukuyama, *Trust: the Social Virtues and the Creation of Prosperity,* Penguin Group, London, 1995, p. 197.

[4] UNESCO, *Right to Universal Access to Information in the 21st Century,* Infoethics 2000 Congress, Third UNESCO Congress on Ethical, Legal and Societal Challenges of Cyberspace, 13-15 November 2000.

[5] Fukuyama, *Trust: the Social Virtues and the Creation of Prosperity,* p. 195 and p. 321.

8.2 Legal and social relationships online: identity, trust, and authenticity

The concept of a legal relationship is one way of considering how trust (or the lack thereof) affects electronic transactions and how it underpins the Internet as a community. The problem of trust in online transactions is complicated by the number of additional actors that are involved in recordkeeping processes outside of a closed community. It is not just the sender and the recipient that need to be trusted, but also those providing the authentication of the identities to the transaction, as well as network providers and the telecommunications infrastructure. In electronic commerce transactions there are several third parties involved that may interfere in the transaction and this may occur outside of the jurisdiction of the legal system in which the transaction occurs.

In 1998 the Australian Electronic Commerce Group report identified the key issues to facilitate electronic commerce as mechanisms 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 report found that commercial relationships have worked in a bounded context, for example within the banking community because of commercial practice, and that the lack of a pre-existing relationship between two parties transacting on the Internet prevents electronic commerce developing.[6] The requirement of pre-existing trust is also the basis of social relationships. The transactional perspective of recordkeeping involves author-actor (sender) and recipient identity that may or may not be part of a pre-existing relationship, that is the sender-recipient are not known to each other. Relationships built around author and addressee in particular, have reappeared in the 'web of trust' authentication technologies.[7]

Although global markets are a feature of electronic commerce, closed electronic markets also use Internet technologies, for example the stock exchange or the pharmaceutical industry. The 'whole of government' online, from business to business, as well as business to consumer, is based

---

[6] Attorney-General's Electronic Commerce Expert Group, *Electronic Commerce: Building the Legal Framework,* Report of the Electronic Commerce Expert Group to the Attorney-General*,* 31 March 1998.

[7] Clifford Lynch, 'Authenticity and Integrity in the Digital Environment: An Exploratory Analysis of the Central Role of Trust', in *Authenticity in a Digital Environment*, Council on Library and Information Resources, Washington, D.C., 2000, pp. 32-50.

on the level of trust that exists between citizen and state. These are either 'closed' or 'semi-open Internet systems'. Professional relationships operate as 'closed' intranet systems for reasons of confidentiality. Industry groups continue to operate as communities bound by their own regulatory frameworks, which can be identified using the juridical or warrant-based recordkeeping models. The 'closed' intranet system is preferable for most business contexts (see below: Accreditation schemes).

The nature of legal and social relationships is also indicative of which Internet technology best provides for retaining trust and reliability that must be captured and retained by recordkeeping systems. Legal and social relationships applied to the Internet context require identity and trust to continue to operate within communities of interest. These communities already have their own mechanisms of control, such as professional authorities that provide certification of professional identity, that need to be integrated into networked systems.

8.2.1 Authentication technologies

With the commercialisation of the Internet, protecting person identity has become a key issue. Encryption, originally used to ensure the integrity of the message,[8] moved to authenticating the participants in transactions by adopting electronic signatures.[9] However, electronic commerce models

[8] Richard C. Barth and Clint N. Smith, 'International Regulation of Encryption: Technology Will Drive Policy', in *Borders in Cyberspace*, Information Policy and the Global Information Infrastructure, eds Brian Kahin and Charles Nesson, MIT Press, Cambridge, Mass., c1997, p. 283. Encryption was adopted by the financial industry in the 1970s for secure payment systems, and the rest of the private sector followed. Encryption has been regulated in the United States to protect foreign intelligence and law enforcement interests.

[9] Electronic signatures are a form of technology which enable the sender of an electronic document to create an electronic signature. When communications are between closed groups the signature is validated by the network operator, while in open communications validation depends solely on the technology. In non-technical terms electronic signature technologies link the information content of the document to some unique information which only the signatory possesses. This might be an encryption key stored in a storage device, for example on a hard disk or a smart card, biometric data, such as the signatory's thumb print, voice and retina print, or hand-written signature metrics. Chris Reed, *Internet Law: Text and Materials*, Butterworths, London, 2000, pp. 154-164.

limit authentication of parties to the immediate transaction.[10] Verifying the authenticity of records 'over time', means that encrypted data has to survive technology migrations. Authentication technologies such as key authentication are software and/or hardware dependent, and encrypted records and signatures may become unreadable without the appropriate software.[11]

Public key cryptography

Public key infrastructure includes public key cryptography, digital signatures,[12] certification authority software, certificates, and staff who enforce policies, procedures and practices.[13] These are the procedural controls necessary for trustworthy records that are also part of recordkeeping and archival practice.

Public key cryptography involves pairs of matching keys: one public and one private. Messages signed with the private key can be validated with the public key, but the public key cannot be used to create a signature for a new message. The signature is kept secret by adopting asymmetric cryptography which uses both a public and a private key. In order to validate a digital signature, the recipient needs to know both the public key of the signatory and the encryption system used to form the signature.

Trusted third party: certification authorities

If the parties have not had previous dealings, the recipient will have no knowledge whether the public key does in fact correspond to the purported

---

[10] The authentication of the parties at the time of the transaction does not mean that the record will remain authentic over time, unless specific measures are taken to preserve the record. See current recordkeeping research in the archives and records community on the preservation of authentic and reliable electronic records over time in Chapters 2 and 4.

[11] Gail L. Grant, *Understanding Digital Signatures: Establishing Trust over the Internet and Other Networks,* McGraw-Hill, New York, c1998.

[12] Digital signatures are electronic signatures which are based on public key cryptography. The European Directive 1999/93/EC covers electronic signatures in its widest term but most of its provisions deal with digital signatures. See Jos Dumortier, 'Directive 1999/93/EC on a Community Framework for Electronic Signatures', in *eDirectives: Guide to European Union Law on E-Commerce*: *Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection,* eds Arno R. Lodder, Henrik W.K. Kaspersen, Kluwer Law International, Dordrecht, 2002, pp. 33-34.

[13] Grant, *Understanding Digital Signatures,* p. 44.

identity of the signatory. It requires a digital identification certificate issued to an individual by a trusted organisation, a 'certification authority' (CA) that can vouch for an individual's identity. The certificate binds the identity of an individual to a public key. The certificate is stored in a computer by the user, to be incorporated with an electronic signature, using software for this purpose. A certificate will contain a copy of the public key, information specific to a user, information on the issuer, and a validity period. A message with the accompanying certificate provides the evidence from an independent third party that the person named in the certificate did in fact have access to the unique signature data, so long as the public key included in the certificate validates the signature. In the absence of evidence from the alleged signatory that some third party 'forged' the signature, this evidence should satisfy a court.[14] Certificates are used for different web-based applications.[15] A certificate from a trusted CA endorses the rightful owner of the keys. Every time a transaction takes place, a public key is sent to the service provider together with a copy of the digital certificate. If the service provider trusts the CA that issued both the certificate and the key, it should trust the customer. The service provider repeats the process from his/her end, so that each party ends up with a certificate authenticating the other, and the other party's private key.

Digital signatures are also used for authorisation, to ensure a party is sanctioned for a particular function, which protects privacy or confidentiality of the content, data integrity (proof that the object has not been altered), and non-repudiation (protection against someone denying

[14] Andrew P. Sparrow, *The Law of Internet & Mobile Communications: the EU and US Contrasted,* tfm Publishing Ltd, Harley, England, 2004, p. 123.

[15] The establishment of third party certification authorities in Australia has included Australia Post (which has since closed its operations as they were not profitable), KPMG and Security Domain. Types of services provided include web server certification where the certification authority (CA) checks the authentication of the company owning the server against national company databases and the domain name registry. An ongoing responsibility of the CA includes monitoring servers that have been authenticated. The certificate once issued sits on the web server as a text file and can be viewed via an icon on the browser. It will state that it has been issued by KPMG and Dun and Bradstreet the company information compiler. Security Domain issues certificates but does not carry out the authentication process. For example the Australian Medical Association sends in a digitally signed request to KPMG and acts as the Registrar, the traditional authorisation role of the 'legal author' of the records. Some organisations act as authentication bodies for their own systems, for example the Australian Taxation Office. Sue Lowe, 'Keys to the Kingdom', *The Age*, 22 September 1998.

they originated a communication or data). For example, credentialing passports depends on a third party (the government) which issues the credentials, trusts in the ability of the third party to authenticate properly, and makes it difficult to forge or modify the credentials.[16] Public key cryptography operates on third party trust, which in archival science emanating from the public records tradition has been the government.

Accreditation schemes

Certification includes a process of identification via a chain of trusted persons, defined as 'Certification Path Discovery and Validation'.[17] English courts have accepted the concept of authentication of message origin via a train of trusted messages.[18]

---

[16] Grant, *Understanding Digital Signatures,* p. 20.

[17] Reed, *Internet Law: Text and Materials,* pp. 128-131. If an authentication certificate emanates from a CA who is already known to the recipient, and whose public key is in the possession of the recipient, that key can be used to check the validity of the certificate. The recipient's software decrypts the certificate's signature with the CA's public key, and if the result is meaningful this will provide strong evidence that the certificate was issued by the CA, and that the level of identification stated in the certificate has been undertaken by the CA. If the recipient does not know the CA, he can use the CA's own ID Certificate, which is incorporated in the holder's certificate, to check the true identity with the issuer of that ID certificate. If that issuer is also unknown, its identity can be checked via another ID certificate, and so on, that is, as a chain of identity. Whenever a CA is identified, that CA's public key is added to the recipient's list of known CAs. Thus when in future an ID Certificate is encountered which has been issued by that CA, the recipient need undertake no additional checking. There is a limited period of validity for an ID certificate. A certificate could be revoked because of loss of control over a private key or a change of status, for example new employment. The CA issues an electronic notice for revocations (CRL), held in a public repository or with the CA.

[18] In *Standard Bank London Ltd v Bank of Tokyo Ltd* (1995) 2 Lloyd's Rep 169, the defendant communicated with the plaintiff by trusted telexes containing secret codes known only to sender and recipient. Because the parties did not have a trusted telex relationship between themselves, the defendant sent his messages to a correspondent with whom he did have such a relationship, and that correspondent forwarded them to another intermediary who passed them on to the plaintiff. The case was decided on the basis that these messages were properly authenticated as originating from the plaintiff, and the expert evidence (accepted by the court) stated that trusted telex messages were treated by banks as if they were signed by the sending party as standard business practice. Ibid., pp. 129-130.

The authentication infrastructure has both legal and ethical elements. The CA has to be trusted to take proper evidence of the holder's identity if he/she issues ID certificates and the CA has to employ honest staff. There has to be an independent certification that the CA adhered to appropriate technical and operational standards, to verify that the certificate has been assessed as meeting certain security assurance criteria.[19] The emerging trend is to establish voluntary accreditation systems that monitor an accredited CA to ensure continued compliance with standards.[20]

Most accreditation schemes give CAs power to recognise ID certificates issued by foreign CAs as having equivalent legal effect to certificates issued by a domestic, accredited CA. Thus accreditation of CAs is not mandatory but it is essential to have full legal effect.

The global ID Certificate infrastructure is likely to become a fundamental part of the global communications infrastructure and will take into account:

- whether the CA is a fit and proper person to act (an ethical element),
- whether the organisation is financially well-established so as to be able to continue its operations and meet its obligations,
- whether its staff are properly qualified and adequately trained and supervised, and
- whether its technical systems are of sufficient quality, and adequately maintained.

The CA must demonstrate a high level of competence in the identification of applicants for a certificate, the secure generation and management of signature keys, the maintenance of security and confidentiality in respect of its records, and the maintenance of proper records for the required periods of time.[21] These requirements are met from a range of self-regulatory schemes as well as legislation which specifies the accreditation requirements in detail, including auditing the CA.

The CA 'authorises' the act, an essential element in record creation and its reliability, by 'binding' the owner to their authenticators. This is why

---

[19] Ibid., pp. 130-131. Examples of independent certification include the European Commission's certification processes or the 'common criteria certificate' issued by a certification body.

[20] Ibid., p. 130. Accreditation was until recently linked with key escrow for law enforcement purposes. A CA, as part of the accreditation process, was meant to retain a copy of the encryption keys and provide them to law enforcement agencies in prescribed circumstances. This has been criticised widely and is no longer linked to accreditation schemes.

[21] Ibid., p. 133.

licensed third party CAs should operate within a hierarchical structure of checks and balances by other CAs.

Public key infrastructure requirements vary per 'community'. A network of trust consists of a group of CAs that a business decides to trust for the issuance of certificates for a specific purpose.[22] In an 'open system' consumers obtain a single certificate from a third party CA to use with many parties, while in a 'closed system' a special purpose certificate is issued, for example only between the government and a citizen.[23] Roles in cyberspace can be delineated by information tagged to a record; for example, employee identification in a digital certificate provides both the employee's identity and his/her authority much the same way as competencies and delegations are used in diplomatics to identify record 'authors'. Professionals who undertake activities on the Internet can be identified globally with digital certificates tagged to their transactions with clients. Thus current public key technology supports professional, commercial and government relationships 'in time'.

8.3 Internet recordkeeping participants: roles and socio-legal relationships

8.3.1 Participants in Internet regulation

Internet regulation can be analysed in terms of the legal and social relationships of business participants involved in web activities, from the service providers, the users, the parties to the business transactions, trusted third parties and the technical infrastructure. The boundaries of regulation can be delineated by looking at national boundaries, but the international nature of the Internet makes it necessary to keep a global perspective in mind.

---

[22] Grant, *Understanding Digital Signatures,* pp. 39-45; pp. 54-55. A bank account identification process is used to authorise someone to take payments from that account. In a network the bank issues the account holder a certificate via their certification authority. The account holder sends a request for a letter of credit to its bank, signing the request. A bank sends a digitally signed letter of credit to the seller's bank, guaranteeing payment upon receipt of goods. The seller's bank can verify the identity of both the bank and the buyer through their certificates.

[23] Adrian McCullagh and Ian Commins, 'Cryptography: From Information to Intelligent Garbage with Ease', in *Going Digital 2000, Legal Issues for E-commerce, Software and the Internet*, eds Anne Fitzgerald, et al., 2nd edn, Prospect Media, St. Leonards, New South Wales, 2000, pp. 212-213.

The function of a record as a right-duty 'thing as relationship' which encapsulates the rights and obligations of recordkeeping participants does not alter in online transactions. Trusted third parties acting either as intermediaries or as accountability mechanisms have always been essential to record authenticity. However, there are new intermediaries who perform various roles necessary for trustworthy transactions on the web. In theory existing entities can take on these roles, for example in the government sector archival authorities could become certification authorities, registrars of births, deaths and marriages could retain certification certificates, and in civil law systems notaries could take on a similar role in private transactions.[24] The fact that they have not taken on these roles means that authenticity over time may be compromised.

The notion of a legal person that has the capacity to act legally does not change in the online environment. Legal persons have always been conceptual or 'virtual' personae.[25] What is relevant is the capacity of legal persons to enter into legal relationships. Conceptually the theory of legal relations is not restricted to territorial theories.[26] Even if remedies for actions are different in the online context there are still similar sanctionable legal relations.

8.3.2 Recordkeeping participants as moral agents in the web environment

Ethical theories in the open Internet context are difficult to replicate. For example, the ethical demand depends on one-to-one personal relationships amongst strangers. Virtue ethics depends on closeness and familiarity, which can engender pity and other emotions.[27] Cultural-relativist positions

[24] Anne Picot, 'Uncovering the Mysteries of Digital Signatures. A Discussion of What Signatures Really Stand for and How They Should be Managed in the Digital Environment', in *Convergence, Joint National Conference, Conference Proceedings*, the Joint National Conference of the Australian Society of Archivists and the Records Management Association of Australia, 2-5 September 2001, Hobart, p. 259. See the legal status of Internet participants within socio-legal relationships, and Fromkin's 'cybernotary' later in this chapter.

[25] Person (persona) is any entity to which the law attributes a capacity for legal relations. Albert Kocourek, *Jural Relations*, 2nd edn, The Bobbs-Merrill Company, Indianapolis, 1928, p. 76, footnote 3.

[26] Ibid., p. 236.

[27] Michael Stocker, 'Emotional Identification: Closeness and Size: Some Contributions to Virtue Ethics', in *Virtue Ethics, A Critical Reader,* ed. Daniel Statman, Georgetown University Press, Washington, D.C., 1997, pp. 118-127.

can only be sustained if a community remains 'closed'. Ethical relationships could be built up over time in professional relationships, but would not operate for one-off business relationships, or in the government context. Amongst ethical theories, Kant's notion of relations between strangers provides the best adaptation to the online world.

Depersonalisation of responsibility in the electronic world creates a greater need for personal ethical systems. 'Intelligent' agents and computer programs that make 'decisions' for individuals challenge the notion of personal and corporate responsibility as necessary to business actions. No legal system can operate without personal attribution for action. Role, linked to identity, is probably one of the most important issues in the online world (see above in relation to authentication). The issue of deception is both a legal and a moral issue.[28] The Internet provides users with an illusion of power and control and the means to separate themselves from their behaviour.[29] In neo-Kantian thinking a computer system is said to act 'intentionally' but 'not intelligently', and therefore cannot be considered to have self-conscious causality.[30] Ethical theories that support a rational self-conscious control over activity cannot sustain the development of the 'self-managing' record.

8.3.3 Recordkeeping participants as legal actors in the web environment

The notion of legal participants involved in the creation of records can also apply to Internet actors. Even a simple transaction on the web involves many actors.[31] For example, accessing a web page involves the controller of the resource, the resource host, and the user. Many of the activities are not the result of conscious human decisions, but neither are they automatic. The most important aspect is to identify the principal actors and their roles, and the rights and liabilities that flow from these roles.

---

[28] John L. Fodor, 'Human Values in the Computer Revolution', in *Social and Ethical Effects of the Computer Revolution,* ed. Joseph Migga Kizza, McFarland & Company, Jefferson, N.C., 1996, pp. 256-266.

[29] Paul C. Grabow, 'La Technique: An Area of Discourse for Computers in Society', in *Social and Ethical Effects of the Computer Revolution,* ed. Joseph Migga Kizza, McFarland & Company, Jefferson, N.C., 1996, pp. 298-312.

[30] Christine Korsgaard, Professor of Moral Philosophy, Harvard University, 'Human Action and Normative Standards', Guest Lecture, the Australian Catholic University, Christ Lecture Theatre, Melbourne, Friday 14th of July 2000.

[31] Reed, *Internet Law: Text and Materials*, Chapter 2.

There are two basic groups involved in an initial Internet exchange: the parties to the exchange, and the intermediaries or hosts that receive and pass on the packets.[32] Hosts use a common set of protocols, that is, each host accepts to transmit packets addressed to others. The interconnection agreement between any pair of hosts is a private one, and obligations, including charging will differ widely. Multiple actors can have possession and control of data on the Internet.

Infrastructure providers are the communications carriers in Internet transactions. The facilitating infrastructure or intermediaries include transmission hosts, resource hosts or website hosts. The primary controller is the website proprietor, but the resource host retains ultimate control and can delete and prevent access to files subject to the contractual terms of agreement with the subscriber. The web host has possession of the resources and some control over them; someone authors the material and may own the copyright. A user accesses the site and copies material into his/her computer's memory. The server may be under one domain name but a virtual site may link to a set of networks and reside in several countries.[33]

Communication services include the Internet service provider (ISP) that connects to other hosts and provides access, mailbox, and disk space for resource hosting. Directory services and transaction facilitation services include domain name allocation and identity services.

There are a small number of pre-existing relationships, but most are indirect relationships passing through hosts. Internet intermediaries more commonly have no pre-existing relationship with each other. They may provide services to one or more of the parties, including communications services such as access or information storage. Other services include identifying one of the parties.

The following is a useful breakdown of Internet actors.[34]

---

[32] 'Internet Access Categories' as produced by the Internet Society in 1995, quoted in Reed, *Internet Law: Text and Materials*, p. 9.

[33] Ibid., p. 19.

[34] Internet actors and roles are drawn from Graham J.H. Smith et al. (eds), *Internet Law and Regulation: A Specially Commissioned Report,* F.T. Law and Tax, London, 1996, Chapter 1, 'Overview of the Internet', with additions.

Infrastructure/network provider: provides the physical connections; and links to the infrastructure of the Internet, routers, hosts and pipes, that is, telecommunications, governments, and networks.
Service provider/access provider (ISP): provides a range of access services, including client software; dial-up or broadband accounts for home use; mailbox space; permanent connections for commercial use; and web hosting and design.
(Resource) host: provides the storage space accessible via the Internet; the servers; may be involved with placing material on the host; may run newsgroups; and provides domain name server
Administrator: provides Internet protocols and domain names.
Content provider: whoever is placing content on the web; for example companies, individuals; linkages to other sites.
Navigation provider: sifts the content using 'search engines' or provides directories.
Transaction facilitators or intermediaries: provide security and identification of the parties to the transaction; act as trusted intermediaries, for example CAs. See also the 'cybernotary', recordkeeping professionals and archival authorities.

Internet participants include persons (physical or legal) that form part of the transaction or that have rights or obligations as a consequence of that transaction. From a recordkeeping view the list below adapts the Internet actors listed above with familiar recordkeeping actors, as well as new ones or old ones in new guises. The first four entries below are participants that were introduced in Chapter 4.

Competent author: the person having authority to carry out an act; an entity/corporate body capable of acting legally. The identity of the facility or location from which the information has originated, a 'facility identifier.
Recipient/addressee: the name of the person(s) to whom the record is directed or for whom the record is intended.
Third party/ transaction facilitator or intermediary: the 'preserver' or professional registration bodies.
Record or data subject: the person who is the subject of, or referenced in a transaction; that is, referenced in the content or subject matter of the transaction; may have statutory rights of access or privacy and confidentiality protection.
Service provider: the provider of a range of access services, including client software; services include dial-up and broadband 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.
Internet regulators: government authorities; legal and social enforcement mechanisms.

The third party sits outside the transaction but has rights because of the relationship with the first and second parties as a result of the consequences of the transaction. In the Internet context third parties include recordkeeping professionals, or transaction facilitators, that is, authenticators, such as CAs, the 'cybernotary',[35] 'gatekeeper'[36] or archival authorities in their primary role of trusted third parties. The concept of the cybernotary, a

[35] Froomkin, 'The Essential Role of Trusted Third Parties in Electronic Commerce'.

[36] The Gatekeeper's role is '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'. '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 have played the role of gatekeeper? See *Gatekeeper: A Strategy for Public Key Technology Use in the Government,* Office of Government Information Technology, Canberra, 1998.

trusted third party that provides a guarantee or certificate for each transaction has links to that of a legal notary, one the oldest recordkeepers in society, and also a role played by archival authorities as the independent third party for public records deemed of long term value. A cybernotary would also provide a means overcoming the differences between the civil and the common law systems when authenticating online transactions.[37]

In Figure 10 Internet participants are represented in an Internet regulatory model of legal relationships. The use of broken lines in the figure denotes a tenuous relationship between the service provider and the actors involved in the transaction.

A participant on the Internet, defined as moral or legal agent, can have a number of roles. When determining the legal consequences of activities on the Internet, it is important to identify which role the person is performing, for example a service provider may perform the same role as the network provider, host and access provider. It is necessary to identify the role and the legal activity involved. The fact that a telecommunications carrier may 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.

[37] 'CyberNotary would be a lawyer able to demonstrate that she has the ability to issue certificates from a trusted computing environment. The hope is that civil law jurisdictions will come to accept a CyberNotary's certification as legally sufficient authentication and recordation of legal acts executed in the United States. If so, a power of attorney or the transfer of corporate shares certified by a CyberNotary in the United States would be recognised and enforced in those jurisdictions, even when an ordinary United States lawyer's or United States notary's certification would not suffice.' Froomkin, 'The Essential Role of Trusted Third Parties in Electronic Commerce', pp. 7-9.

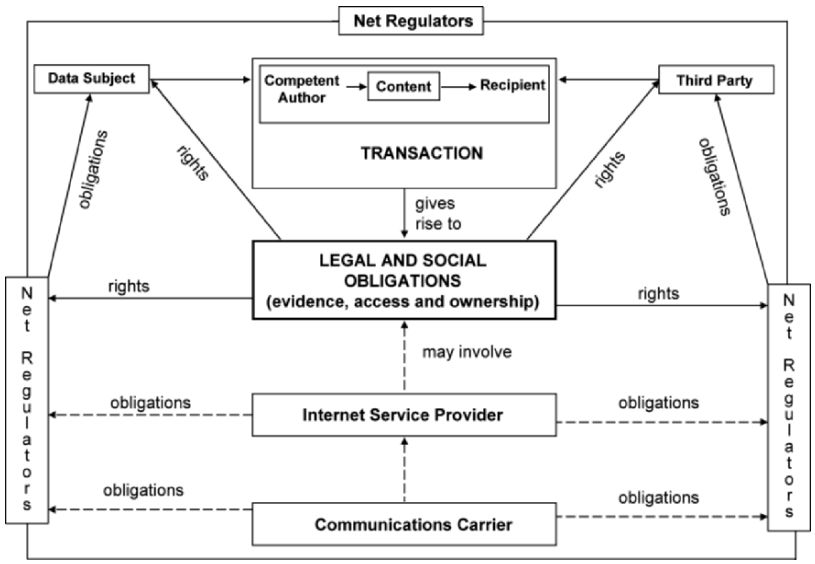

Fig. 10 Legal Relationship Model: Participants in an Internet Transaction

Different actors in an Internet 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 and other rights. In an intranet context, the ownership can be attributed to an organisation, which is likely to be vicariously liable for the content, if it is in breach of a law, unless the act carried out by an employee is outside of the scope of his/her employment.[38] There is therefore a need to identify the legal relationships between Internet actors, for example:

- The relationship between the website 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 Internet.

[38] Anthony Willis, 'Intranets and the Law', in *Intranets: Problems and Opportunities for Recordkeeping, Proceedings Conducted by the ACT Branch of the Records Management Association of Australia at Parliament House, Canberra, 10-11 March 1999,* ed. Anthony Eccleston, Records Management Association of Australia, ACT Branch, Canberra, 1999, p. 45.

- The relationship between the end user and the ISP would include the extent of liability the ISP takes for the end user's transactions on the Internet.

How far the actors can be regulated using existing national laws and what other rule sets apply to the enforcement of rights and obligations on the Internet have been slowly emerging.[39]

8.3.4 Proprietary rights of Internet participants

Protecting proprietary information will depend on the nature of the relationship and the activities in which Internet participants are involved. For commercial relationships, a link to the competencies in the organisation, that is, who is responsible for particular activities, is also needed to clarify liability.

In the Internet context the owner's copyright in a 'work' and a record's integrity are threatened when a communication is first transmitted (interception and alteration). From this perspective moral rights legislation is particularly relevant as it seeks to protect the integrity of a work. In diplomatics the 'moral rights' author is the 'writer' rather than the author of the work as defined in legislation.

The ISP has obligations to prevent copyright breaches and to protect rights of the author to communicate to the public.[40]

8.3.5 Privacy rights and obligations of Internet participants

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 ISPs 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 may have to compromise the privacy of their clients in order to comply with this aspect of copyright.

Legal and social relationships based on trust and the duty of confidentiality have been a major source of protecting the privacy of parties to a transaction. In the online environment participants in an

---

[39] See Chapter 7.

[40] David Brennan, 'Simplification, Circumvention, Fair Dealing and Australian Copyright Law', in *Going Digital 2000, Legal Issues for E-commerce, Software and the Internet*, eds Anne Fitzgerald, et al., 2nd edn, Prospect Media, St. Leonards, New South Wales, 2000, p. 108.

Internet transaction may be strangers, however if identities are known then trust between parties increases. The link between identity and trust is based on having access to knowledge about the person with whom one is dealing; trust increases if moral views, professional standing, and reputation of the organisation represented are known. Contract and other laws serve as a backup when trust fails.

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 parties to the transaction or record/data subjects, for example held by ISPs or authentication certificate providers (record identity).[41] For electronic commerce a unique identifier may emerge for a global context. The use of a unique identifier (such as a business number) could be used to link data across networks and depends on trusted third parties.

Privacy needs to take into account players such as ISPs, CAs and archival regulatory authorities operating as trusted third parties, essential to legal and social relationships online.

8.3.6 Evidence for establishing rights and obligations of Internet participants

Electronic commerce legislation may include provisions which support recordkeeping processes and actions online, needed to establish the rights and obligations of parties in a legal and social relationship. For example the Australian *Electronic Transactions Act* 1999 (Cth) includes rules to determine the time and place of dispatch and receipt of electronic communications and their attribution, so that participants in a transaction can be uniquely identified, essential for contract formation but also for recordkeeping reliability and authenticity.

The relevant recordkeeping provisions in the Act include identifying consenting parties to a transaction, that is, the author-authentication link in recordkeeping. For example the document has to be signed. In s 10 the 'signature' must identify that person sufficiently for the purposes of that communication, it must indicate the person's approval of the contents of

[41] *Privacy Act* 1988 (Cth), 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 (CAs) would be limited in how they use or disclose at least some identifiers which they would have a primary purpose in collecting.

the communication, and the signature method must be as reliable as appropriate for the purposes for which the information was communicated.[42] Section 15(1) provides that a person purporting to be the originator of an electronic communication will only be bound by the electronic communication if in fact the electronic communication was sent by that person or with their authority.

Other recordkeeping provisions include creating and capturing the document into a system. Sections 9(1) and (2) allow a person to satisfy a requirement or permission to give information in writing under a law of the Commonwealth by providing that information by means of an electronic communication, subject to the general condition that, at the time the information was given, it was reasonable to expect that the information in the form of an electronic communication would be 'readily accessible so as to be useable for subsequent reference'.[43] There is also a requirement to retain reliable and authentic electronic records that have identifying metadata required by law if it is a 'reasonable' expectation that the electronic communication would be subsequently accessible. Section 12 requires an electronic communication which under Commonwealth law is required to be retained for a particular length of time to be retained in electronic form if it is reliable, that is, it includes information to identify the record, which includes its origin, destination, time of dispatch and receipt. Recordkeeping metadata on time and place of receipt of a transaction is in s 14. Default rules determine when, and from where, an electronic communication is sent and when and from where it is received. Parties may agree to vary these rules to determine the time and place of dispatch and receipt in their dealings with each other.[44]

---

[42] 'The intention of clause 10 is to allow a person to satisfy a legal requirement for a manual signature by using an electronic communication that contains a method that identifies the person and indicates their approval of the information communicated. This method by which a person is identified electronically is commonly called an "electronic signature". However, the choice of a particular method must be as reliable as appropriate in the circumstances. In addition, where a person must provide a signature to a Commonwealth entity the person must comply with any information technology requirements in relation to the signature method. Finally, where the signature is required to be given to a person who is not a Commonwealth entity, that person must consent to the use of that signature method.' From Australia, Senate, *Revised Explanatory Memorandum, Electronic Transactions Bill 1999,* 30 June 1999, pp. 30-31.

[43] Ibid., p. 26.

[44] *Time of dispatch and receipt* in subclauses (1) and (2): '… of dispatch is deemed to occur when the communication enters the first information system outside of the control of the originator. For example, a message sent by the originator may

The *Electronic Transactions Act* 1999 (Cth) requires parties to consent to the transaction, but how this affects other third parties, including archival authorities, is not covered in the legislation. Both evidence legislation and electronic commerce Acts need to be read with archival Acts in relation to preserving records over time.

8.4 Legal liabilities of Internet participants

8.4.1 Proof of identity

The liability of transaction facilitators for incorrectly identifying a person is a key issue in electronic commerce.[45] Chris Reed argues that in the physical world few transactions require formal evidence of identification as a standard procedure. The establishment of specialised third parties whose function it is to issue identification tokens has been an important feature of Internet transactions and has arisen in the context of the signing of electronic documents.[46] In archival science, identity data in archival and registry systems has been a mandatory aspect of record identity.

An order to enforce the signatory's legal obligations by proof of an electronic signature, has to demonstrate that in fact it originated from the purported signatory, and could not have been affected by a third party. In the United States the *Uniform Computer Transactions Act* ss 112 and 213 require the party relying on the attribution of the electronic record to establish attribution. Similar attribution provisions are found in the Singapore *Electronic Transactions Act* 1998 s 3. In Australia the onus is on the addressee to prove that a message was sent by the originator or with

---

leave his or her system and enter his or her Internet service provider's system from which it is sent, possibly via other systems, to the addressee's information system. In this situation, the time of dispatch is deemed to occur when the communication enters the originator's Internet service provider's system [not when opened and read]. Unless otherwise agreed between the originator and the addressee of the electronic communication, the time of receipt of the electronic communication is the time when the electronic communication enters that information system'. This is in line with the common law postal rule. *Place of dispatch and receipt*. 'Subclause (5) establishes that the dispatch of an electronic communication is deemed to occur from the originator's place of business and receipt of an electronic communication is deemed to occur at the addressee's place of business'. Ibid., pp. 39-40.

[45] Attorney-General's Electronic Commerce Expert Group, *Electronic Commerce: Building the Legal Framework*, p. 84.

[46] Reed, *Internet Law: Text and Materials,* p. 121.

his/her authority as in common law, that is, the addressee needs to authenticate the originator's identity.[47]

Using the certificate to prove identity

An ID certificate demonstrates that the issuing CA holds identification evidence for its holder, but does not prove that it was in fact the holder who sent the certificate to the recipient. The connection between the sender and holder is made by the electronically signed message which accompanies the certificate. Because the ID certificate also contains a copy of the holder's public key, it can be used by the recipient to check that the signature of the message matches the signature in the certificate. If they match, a presumption can be made that the holder of the certificate is also the sender of the message.[48]

Effects of accreditation

In some jurisdictions, only an electronic signature backed by a certificate from an accredited CA is expressly given the same legal effect as a traditional signature.[49] In some instances electronic signatures act merely as evidence of authentication and approval of a message, but are not specifically stated as complying with the law's formal requirements for signatures.

Liability of certification authorities

What is the liability to the holder of an ID certificate issued by the CA if the certificate contains inaccurate information, so that the transaction fails, or the CA discloses private information about the holder or the key? Given the legal consequences of transactions that would otherwise be difficult to identify on the Internet, the liability on the part of the CA is obvious. The holder and the CA are likely to have a contractual relationship; the liability between them would be managed by contract subject to consumer protection laws or controls on exclusion clauses from which the holder

---

[47] Ibid., pp. 124-125 and p. 212.

[48] Ibid., Chapter 6.

[49] Singapore's *Electronic Transactions Act* 1998, ss 18 and 20 as quoted in Reed, *Internet Law: Text and Materials,* p. 132, footnote 8. See also Italian digital signature legislation which states that only a digital signature which has a public key certified by a CA is legally valid. Dumortier, 'Directive 1999/93/EC on a Community Framework for Electronic Signatures', p. 37.

benefits. These elements are clarified in some electronic signature legislation.

The liability of the CA for losses caused by reliance on a certificate which contains incorrect information is defined and limited where a CA is accredited. Losses suffered by a person who relies on the certificate, 'the relying party', may be defined in accreditation regimes. An unaccredited CA would be subject to general law. It may be possible in common law countries to construct a contract on the basis that the CA had made a unilateral offer to the whole world promising certain things to any person who accepted the offer.[50]

What is the duty of care of a CA when issuing a certificate in terms of verifying the person's credibility? The CA owes the relying party a duty to take reasonable care in ascertaining the accuracy of the information contained in the certificate, and if he/she has failed, he/she would be responsible for the relying party's losses. Tortious liability based on the CA's negligence in ascertaining the accuracy of the information in the certificate may ensue.[51]

Statutory liability regimes usually apply only to accredited CAs. These are based on negligence in ascertaining correctness of information. The CA defines liability in a certification policy statement he/she accepts and is strictly liable for failure to comply with published procedures for ascertaining the correctness of the information in the certificate or for the accuracy of the information itself. Generally the liability is limited to the reliance limit in the certificate itself.[52]

Global consensus is emerging that accreditation enhances legal effectiveness, and liability is defined and/or limited. Foreign accreditation needs to be recognised as equivalent to the domestic law where certificates are used. Most liability regimes agree that reliance limits set out in a certificate should be enforced. CAs can then calculate their liability.[53] Third party liability has been limited for identification services, particularly for communications with legal consequences.[54]

---

[50] See case law in Reed, *Internet Law: Text and Materials*, p.132.

[51] Ibid., p. 139. Duty of care requires a sufficient relationship between the CA and the relying party for a duty to arise. Product liability may be more relevant. Even if tortious liability can be established under applicable law, neither contract nor tort liability covers all the losses suffered by a successful plaintiff, and liability is limited to foreseeable losses, to what is stated in the certificate, and direct loss only.

[52] Ibid., pp. 145-146.

[53] Ibid., pp. 146-147.

[54] Ibid., pp. 82-83.

8.4.2 Internet service providers: legal obligations

The difficulties of enforcement of judicial orders over transaction actors in other countries increase the pressure to hold intermediaries liable, in particular if the originators remain anonymous.[55] The ISP as the 'secondary' actor is often easier to identify than the primary actor.[56]

Liability by ISPs for the illegal activities of their clients may depend on the activity. In an Australian defamation case an Internet provider was sued for defamation after allegations that a London academic had a psychiatric illness were published several times on its service. It was settled out of court for A$10,000 without the ISP admitting liability. The author was also sued. It demonstrates that ISPs are potentially liable for copyright across international borders.[57]

A contractual relationship is usually between the communicating party and its ISP, but unfair contract terms and consumer protection laws in many jurisdictions could render the terms void. Most users will have an express contract which will include ISP liability for communication failure; if there is no contract most jurisdictions will imply that the ISP must take reasonable care in the provision of services to its user. The only way other intermediaries owe an express duty is through an implied contract to all participants and this is unlikely. An enforceable contractual obligation for the benefit of a third party might create a contractual duty owed by a transmission host to the customers of those ISPs with which there is an express interconnection agreement, for example if the ISP

---

[55] Henry H. Perritt, Jr., 'Jurisdiction in Cyberspace: the Role of Intermediaries', in *Borders In Cyberspace: Information Policy and the Global Information Infrastructure,* MIT Press, Cambridge, Mass., 1997, p. 166; pp. 179-184.

[56] Brian Fitzgerald, 'Internet Service Provider Liability', in *Going Digital 2000*, *Legal Issues for E-commerce, Software and the Internet*, eds Anne Fitzgerald et al., 2nd edn, Prospect Media, St. Leonards, New South Wales, 2000, pp. 309-324. See the *Copyright Amendment (Digital Agenda*) Act 2000 (Cth) on ISP and copyright infringement. In the European context, see Cyril van der Net, 'Civil Liability of Internet Providers Following the Directive on Electronic Commerce', in *E-commerce Law: National and Transnational Perspectives,* eds Henk Snijders and Stephen Weatherill, Kluwer Law International, The Hague, London, New York, 2003, pp. 49-57. The UK *Electronic Commerce Regulations* 2002 (EC Directive F12002No2013) include provisions which limit service providers' liability if they unwittingly carry or store unlawful content provided by others in certain circumstances. See Sparrow, *The Law of Internet & Mobile Communications: the EU and US Contrasted,* p. 90.

[57] The ISP did not respond to the request to have the allegations stopped because it did not want to censor the material. David Passey, 'Internet Provider Pays $10,000 Over Libel', *Sydney Morning Herald,* 14 March 1998.

provides a connection to the Internet on a chargeable basis. The ISP has a duty to take reasonable care in forwarding of packets.[58] Proof of breach would be difficult. A tortious duty of care is even less likely to be imposed on the intermediary. The losses are likely to be financial, and a duty of care is only likely if there is a pre-existing (non-contractual) relationship. Even if a particular intermediary did owe a duty to one or other of the communicating parties, it is not foreseeable that the breach of that duty will cause loss. In common law, if there is an insufficient causal link between the breach and the loss, a duty will be unrecoverable.

Liability for copyright infringement

There are three ways an intermediary can be liable for copyright infringement: via copying, possession, or transmission. ISPs may be potentially liable for content they do not control, because they can prevent further dissemination. United States cases indicate that the more an ISP knows about the illegal matter the more liable he/she becomes.[59] Too much control over content may also lead to authorising an infringement.

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 Internet. In fact the liability of the provider increases with involvement in content selection.[60]

---

[58] Reed, *Internet Law: Text and Materials,* Chapter 4.

[59] 'Netcom case' (*Religious Technology Center v Netcom Online Communications Services* 21 November 1995 ND Cal) deals with liability of a Usenet host. The case involved postings to a Usenet newsgroup on a bulletin board (BBS) connected to the Internet by Netcom, a large Internet Service Provider. A former scientologist posted portions of scientology works to the alt.religion. scientology newsgroup, resulting in an action for copyright infringement. The suit was brought against the former scientologist, the BBS and Netcom. The court considered whether the centre could be held liable for incidental copies made automatically. Netcom was held not to be a direct infringer and not found liable for copyright infringement. Other cases such as in *Playboy Enterprises, Inc. v Frena* the bulletin board owner was found liable for distribution despite the fact that the material had been uploaded by one of the users (see 839 F Supp 1552 (MD FLA, 1993)). From Smith, *Internet Law and Regulation*, pp. 18-19.

[60] Peter Gleeson, 'The Internet, Email and Bulletin Boards: Who's Liable for What?' in *Computers and the Law,* Leo Cussen Institute, Melbourne, May 1996, pp. 1-19.

Copyright owners have been opposed to excluding ISPs from liability. The provision of physical facilities alone excludes liability but not if other Internet services are provided, then the law of authorisation may continue to apply. An ISP and a content provider have to be aware of any infringing copies and show they have taken reasonable steps to stop them. If the Internet host or access provider uses or knowingly permits others to use his/her Internet service to disseminate unauthorised copies of copyright works he/she is in danger of infringement.[61]

Who can be sued for infringement and where did the offence take place? What if there is no copyright protection in that country? For copyright purposes, it is not relevant where the material is published but rather the country where the infringement took place, which is where the material is downloaded. Enforcement requires identifying the infringer which may force the owner of the host computer to disclose the identity of its users.

Despite differences between jurisdictions, most laws impose liability where the intermediary knows or has reason to believe that the information content it transmits is unlawful; and where, irrespective of the intermediary's knowledge, it benefits directly from the transmission.[62]

However, the reasoning is based on physical world transactions where the intermediaries are more closely connected with the parties to the transaction, and have a greater opportunity to assess the respectability of those for whom they act and the nature of their activities. Internet intermediaries can identify the source of the transmission, but in practice this is difficult. Thus the trend is towards granting Internet intermediaries much greater immunities for liability for third party content. Different models across national boundaries create uncertainties. The major problem is the identification of Internet actors, where the geographical and jurisdictional diversity of recipients makes the assessment of liability almost impossible.

Specific copyright liability immunity

The United States' *Online Copyright Infringement Liability Limitation Act*, which is part of the *Digital Millennium Copyright Act* s 512 provides immunity to intermediaries who merely transmit packets, store automatically cached information requested by users, host third party

[61] Ibid., p. 18. In Australia the liability of ISPs was addressed in the Attorney-General's Department and Department of Communications and the Arts, *Copyright Reform and the Digital Agenda*, Discussion Paper, July 1997.

[62] Reed, *Internet Law: Text and Materials,* p. 104.

resources, or provide search and location tools for resources located elsewhere.

ISPs are subject to detailed conditions to have immunity, primarily lack of knowledge, lack of direct financial benefit from the third party activity, and respect for the resource controller's copyright management technologies. Australia also includes a provision for immunity if ISPs take reasonable steps to prevent the infringing act. However, in the United States, ISPs register with the Copyright Office to qualify for limitation from liability for third party claims of infringement.[63]

An additional restriction on copyright immunities in both the United States and the European Union is that an intermediary must not strip out technical rights management information that is used to prove the copyright ownership of the work or to track licensed users.[64]

Other intermediary immunities

Many jurisdictions have introduced extensive statutory and general immunities for Internet intermediaries, to cover copyright infringement and criminal law, as well as civil actions for torts such as defamation.[65]

Immunity is generally lost if the intermediary fails to comply with court orders, such as injunctions to block access or to remove unlawful material,

---

[63] Saba Hakim, 'Copyright and the Liability of ISPs', *Law Institute Journal*, vol. 73, no. 9, Sept. 1999, p. 65.

[64] Reed, *Internet Law: Text and Materials,* pp. 109-110. Australian copyright legislation also prohibits the removal of rights management information. See *Copyright Amendment (Digital Agenda) Act* 2000 (Cth) s 16B on removal or alteration of electronic rights management information.

[65] There is great variation in law on intermediary immunity. The United States, the European Union and Australia have introduced immunities for intermediaries. The German *Multimedia Law* 1998 Art. 5 and the European Union Directive on Electronic Commerce 2000/31/EC OJ L. 178, 17 July 2000, p. 1, provide immunity to both transmission and resource hosts as well as to packet transmitters and cache operators. However, host immunity is lost if the intermediary knows the nature of the information content. Singapore's *Electronic Transactions Act* 1998 s 10 extends immunity to packet transmission and caching, but not to the hosting resource. In Singapore there is liability even if there is no knowledge of the action as the ISP makes a profit from the activity, but in practice it is difficult for the host to monitor clients. Thus European Union and German law is more realistic. From Reed, *Internet Law: Text and Materials* pp. 107-118. Similar principles are set out in the Schedule 5 of the Australian *Broadcasting Services Act* 1992, inserted by the *Broadcasting Services Amendment (Online Services) Act* 1999 which came into force on 1 January 2000.

or he/she exercises positive control over the content, including editing it, or removes copyright management information or if the unlawful nature of the resource becomes known, and he/she does nothing about it. Thus there is overall global consensus on the general principle of intermediary immunity, but variations in implementation.

Privacy and Internet intermediaries

There has been a history of the failure of ISPs to maintain privacy.[66] Privacy obligations imposed on ISPs in Australia are under the *Telecommunications Act* 1997 (Cth). The Act considers participants as either a 'carrier' or a 'service provider', and service providers are either carriage service providers or content service providers. A content service includes a broadcasting service or an online service.[67] Therefore anyone operating a website is a content service provider. Internet (access) service providers are carriage service providers. The primary carriage service provider and the access provider may be different. Access service providers are subject to statutory obligations of confidence on carriers and carriage service providers, but these obligations would not apply to content providers.[68]

'In decisions involving telecommunications carriers, to be a common carrier the entity must not control the content of the message'.[69] Internet service providers and other carriage service providers under the *Telecommunications Act* (Cth) may have different functions, but under the *Copyright Amendment (Digital Agenda) Act* 2000 (Cth) an ISP is defined as a carriage service provider.

Telecommunications providers

An entire regulatory framework for privacy is in place for the telecommunications industry in Australia which places limits on third

---

[66] RealNetworks, an ISP used software to gather details about customers. No legal action was taken against the ISP. Kate Crawford, 'Net Firm "Abused Personal Details"', *The Sydney Morning Herald*, 3 November 1999.

[67] *Telecommunications Act* 1997 (Cth) s 15.

[68] Patrick Gunning, 'Legal Aspects of Privacy and the Internet', in *Going Digital 2000, Legal Issues for E-commerce, Software and the Internet*, eds Anne Fitzgerald, et al., 2nd edn, Prospect Media, St. Leonards, New South Wales, 2000, pp. 217-224. See *Telecommunications Act* 1997 (Cth) Part 13.

[69] Henry Perritt, *Law and The Information Superhighway*, John Wiley, New York, 1996, p. 49. Telstra, the major Australian telecommunications carrier is both an ISP and common carrier, thus it has two roles.

party access to Internet transactions.[70] Apart from the protection of the conversations between individuals, other personal details held on names and addresses are not allowed to pass between carriage service providers (carriers and service providers, see definition above).[71] Part 13 of *Telecommunications Act* 1997, s 276 prohibits the use or disclosure of information including the contents of the communication and personal particulars of any person, with exemptions for law enforcement purposes. There are also privacy industry codes under Part 6 formulated by the Australian Communications Industry Forum which are registered with the Australian Communications Authority (ACA). When a code or a revision is registered with the ACA, the ACA gains powers under Part 6 of the *Telecommunications Act* to give warnings and directions, and impose civil penalties for failure to comply. The business enterprises that would be subject to the privacy code are not only 'carriers' and 'carriage service providers' (Internet access providers), but also 'content service providers', a term that is applied broadly. Hence there are sanctions for some kinds of abuses of personal data in the telecommunications sector.[72]

In the United Kingdom the *Privacy and Electronic Communications (EC Directive) Regulations* 2003 implement the European Directive *2002/58/EC on Privacy and Electronic Communications.*[73] They deal with

---

[70] Holly Raiche, 'Telecommunications Privacy - the Interaction of the Privacy and Telecommunications Regulatory Systems', in *Papers from The New Australian Privacy Landscape,* Faculty of Law, Continuing Legal Education, The University of New South Wales, 14 March 2001, pp. 1-9.

[71] 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 from The New Australian Privacy Landscape*, Faculty of Law, Continuing Legal Education, The University of New South Wales, 14 March 2001.

[72] Roger Clarke, *A History of Privacy in Australia: Current Developments*, 16 December 1999, Xamax Consultancy Pty Ltd, Canberra, 1999. Under the *Privacy Amendment (Private Sector) Act* 2000 complaints for interferences with privacy can go under the telecommunications regime or the Privacy Commissioner. Raiche, 'Telecommunications Privacy - the Interaction of the Privacy and Telecommunications Regulatory Systems', p. 9.

[73] The European Directive, 2002/58/EC on Privacy and Electronic Communications states that log files of ISPs must be erased or made anonymous when they are no longer needed for the purpose of the transmission. Several exceptions are applicable, amongst others, in the interest of national security, defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system. The Belgian Cyber Crime Act obliges ISPs to store all traffic data for at least 12 months. Under the Electronic Communications Regulations (EC

direct marketing and with the limitations on the processing of traffic and billing data, caller identification and directories of subscribers, previously covered in a specific *Telecommunication Directive 97/66/EC*[74] on privacy which supplemented *95/46/EC,* and the *Telecommuncations (Data Protection and Privacy) (Direct Marketing) Regulations* 1998.

Thus the nature of the activity and how the roles of Internet participants are defined in legislation and in different industries affect their liabilities. Their legal and social responsibilities must be contextualised to have meaning.

8.5 Legal and social relationships online: the medical, consumer and government context

Human communities have bonded together on the basis of mutual political, economic and social interests over the millennia. Existing communities of mutual interest are using Internet technologies for business and social interaction. The renewed interest in trusted communities of interest, differing in the level of requisite trust by that community, has implications in terms of the standard of recordkeeping that will be required by new 'bounded' communities. One of the major concerns is that trust may be difficult to cultivate in web relationships amongst 'strangers'. However, the relationships analysed in Chapter 6 clearly indicate that professional,

Directive) 2003, which are the UK implementation of European Directive 2002/58/EC on privacy and electronic communications designed for email and Internet uses, retention of traffic data, that is '… any data processed for the purpose of the conveyance of a communication on an electronic communications network or for the billing in respect of that communication and includes data relating to the routing, duration or time of a communication' is only permissible for limited purposes, for example the end of the period during which the bill may be challenged. In the UK the billing purpose is usually six years plus appeals. Sparrow, *The Law of Internet & Mobile Communications: the EU and US Contrasted,* pp. 93-106.

[74] Article 4(1) of Telecommunication Directive 97/66/EC required appropriate security measures for communications services to be applied by the provider of such services. Security is defined to include the confidentiality of the communications. The Directive was designed for telephone and faxes. See Henrik W.K. Kaspersen, 'Data Protection and E-Commerce' in *eDirectives: Guide to European Union Law on E-Commerce*: *Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection,* eds Arno R. Lodder, Henrik W.K. Kaspersen, Kluwer Law International, Dordrecht, 2002, pp. 126-138.

commercial and governmental relationships have trust elements which are not based only on personal 'knowledge' of the participants but on reciprocal rights and obligations that have evolved over time. Technological tools to ensure trust are unlikely to suffice; yet trust is an essential ingredient for business online. In the legal and social relationship model trusted third parties for professional, commercial and government relationships include professional certification bodies, consumer protection entities, and government accountability bodies. These third parties will continue to provide online trust through authentication processes (see Figure 10A, Legal Relationship Model: Participants in an Internet Transaction: Examples).

Recordkeeping standards that have derived from RKMS, InterPARES and the ISO records management standards provide rule sets in a global environment in which geopolitical legal rule sets have become difficult to apply and enforce. Authenticity standards are contextualised through legal and social relationships, such as the doctor-patient relationship, which operate within communities of common interest, or 'enterprises', for example the medical community. Communities of common interest have both general and specific recordkeeping metadata requirements, and trust channels that operate in a networked context. As legal and social relationships are not tied to organisational structures they provide useful tools for ascertaining rights and obligations in the online environment.

The elements of trust as they relate to recordkeeping, currently captured within professional, commercial and governmental relationships, have not been replaced by technology, but they do require additional regulatory controls. The Australian examples below build on Chapter 6 and include the doctor-patient relationship which operates within the context of the health care 'industry', in which security and person identity issues are central. It operates more securely in a 'closed' intranet system. The buyer-seller and government-citizen relationships function in 'semi-open systems' where trust mechanisms are less communal.

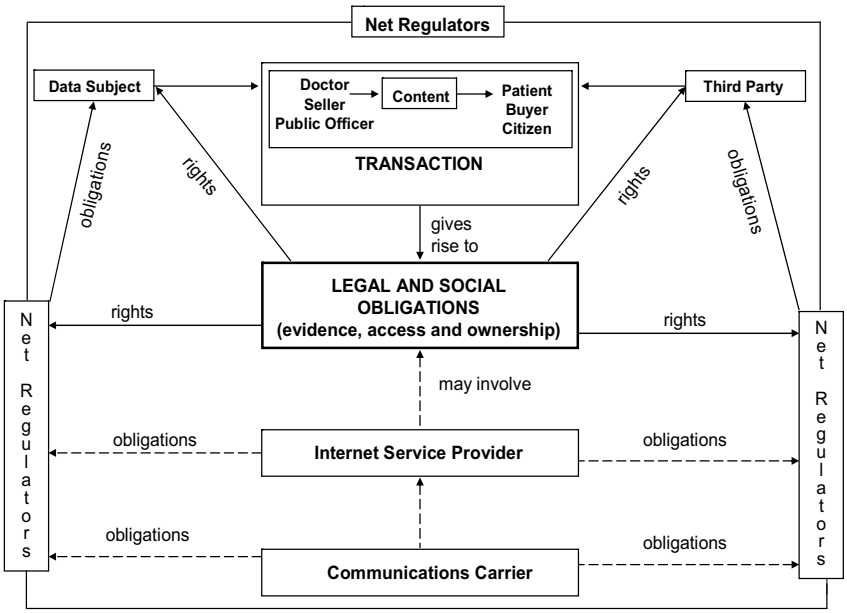

Fig. 10A Legal Relationship Model: Participants in an Internet Transaction: examples

8.5.1 The doctor-patient relationship online

The development of distributed networks, such as the Internet, has made it possible to move many aspects of health care online. In the web environment the integrity, privacy, and confidentiality of electronic medical records becomes of paramount importance. Confidentiality in relationships between health professionals and their clients has a strong ethical basis.[75] The question arises as to whether the traditional ethical approaches are appropriate in the networked environment.

The move to health networking also comes within a 'consumer' centred view of health and the commercialisation of the health industry.[76] The

[75] Ian Kerridge, Peter Saul, and John Mcphee, 'Moral Frameworks in Health Care: An Introduction to Ethics', in *Controversies in Health Law,* eds Ian Freckelton and Kerry Peterson, The Federation Press, Sydney, 1999, pp. 276-289.

[76] 'All About Your Health, Online', *The Age,* 11 May 2000.

doctor-patient relationship is likely to undergo change as a result of both technological and social developments.

Within the increasing interest in national health networks worldwide, the Australian government's *A Health Information Network for Australia: Report to Health Ministers by the National Electronic Health Records, Taskforce* July 2000[77] recommended the creation of Health*Connect,* a joint state health ministers' project, to oversee a nationally coordinated, distributed system of electronic health records. The taskforce identified ensuring privacy and confidentiality as the building blocks of an acceptable system.

International studies on the introduction of an 'EHR'[78] (an electronic health record which is generally defined as a shared health record of an individual) have highlighted the lack of a coherent legal framework for ensuring privacy and preventing its misuse.[79] Improper disclosure of personal medical information may affect a patient's economic interests as well as having social or psychological dimensions,[80] and threaten the

[77] National Electronic Health Records Taskforce, *A Health Information Network for Australia, Taskforce Report*, Commonwealth of Australia, 2000. The National Electronic Health Records Taskforce report is a detailed examination of the issues involved in a national approach to electronic health records. It made a series of recommendations to the state Health Ministers on implementing a national health information network, which formed the basis of Health*Connect,* a major Australian electronic health initiative.

[78] There are a number of definitions of an EHR. From an expansive American Institute of Medicine definition which includes not just patient information but also medical databases, to a United Kingdom restricted definition in which the electronic patient record is the record of care mainly held by the institution, that is, a proprietary record. Flinders University, *The Benefits and Difficulties of Introducing a National Approach to Electronic Health Records in Australia,* Report to the National Electronic Health Records Taskforce, Flinders University, Adelaide, April, 2000 (Appendix), in National Electronic Health Records Taskforce, *A Health Information Network for Australia,* Taskforce Report, Commonwealth Department of Health and Aged Care, 2000, p. 7. The major difference between a medical record and the EHR is that the EHR communicates the record outside of the creation framework. For a list of definitions, see ISO/TC 215 *Ad Hoc* Group Report, *Standards Requirements for the Electronic Health Record & Discharge/Referral Plans*, Draft V 2.1, 31 May 2002.

[79] *A Health Information Network for Australia*, Part A, Chapter 4, discusses several major national initiatives. Differences in definitions of an electronic health record reflect varying cultural medical traditions.

[80] Lawrence O. Gostin, Joan Turek-Brezina, Madison Powers and Rene Kozloff, 'Privacy and Security of Health Information in the Emerging Health Care

continuation of an environment where patients are willing to seek timely medical advice.[81] Moreover, medical care is predicated on access to a reasonably complete set of medical records. These systems create, capture and access patients' records across numerous organisations and link or merge them with administrative health systems for billing, government reporting, and statistical analysis. If the EHR is the complete medical record of a person (some definitions focus on family), it will need to be retained for at least the lifetime of the patient to provide continuity of health care. If it is not the complete record, its relationship with the institutional record needs to be clarified. Therefore, the identity of the author of the records, relevant to its reliability and to its ownership, must be provided with technological, legal and ethical safeguards. The loss of accessibility to, and intelligibility of the records, loss of the original functionality of the data during transfer to a new technology or accidental loss due to media failure (the integrity of the records) are of particular concern.[82] The developments in health networks provide an example of the need to apply the results of recordkeeping research to specific domains.[83]

The implementation of a national health network relies on cooperation and participation of patients and the medical community. If a distributed system of electronic health records is implemented, there is a serious risk that the core elements of the doctor-patient relationship, such as trust, will

System', *Health Matrix: Journal of Law-Medicine* vol. 5, 1995, pp. 1-36; Chari J. Young, 'Telemedicine: Patient Privacy Rights of Electronic Medical Records', *University of Missouri Kansas City Law Review*, vol. 66, Summer, 1998, p. 921.

[81] Michael Kottow, 'Medical Confidentiality: An Intransigent and Absolute Obligation', *Journal of Medical Ethics,* vol. 12, no. 3, Sept. 1986, pp. 117-122; Paul T. Cuzmanes and Christopher P. Orlando, 'Automation of Medical Records: The Electronic Superhighway and its Ramifications for Health Care Providers', *Pharmacy and Law*, vol. 6, 1997, pp. 19-32.

[82] Livia Iacovino, 'Trustworthy Shared Electronic Health Records: Recordkeeping Requirements and Health*Connect*', *Journal of Law and Medicine*, vol.12, no. 1, Aug. 2004, pp. 40-59; Amy M. Jurevic, 'When Technology and Health Care Collide: Issues with Electronic Medical Records and Electronic Mail', *University of Missouri Kansas City Law Review*, vol. 66, Summer 1998, pp. 809-836.

[83] The need to contextualise recordkeeping research results has been an outcome of both the Monash RKMS and InterPARES 1 recordkeeping projects, that is, generic recordkeeping metadata schema and elements of record authenticity have to be applied to domain-specific needs. Recognition of differences in the application of authenticity is also supported by major information peak bodies, such as the US Council on Library and Information Resources, in *Authenticity in a Digital Environment*, CLIR, Washington, D.C., 2000.

be damaged. The networking of health records provides a good example of the need to work within a community of common interests based on trust, and to analyse the issues in terms of identifying the legal and ethical responsibilities of health participants in 'business' transactions.

Regulation of online health services: international context

When a patient's record is transmitted electronically and stored in a number of databases, to be accessed by other health providers, including hospitals and patients, valid consent from patients is required by medical practitioners, organisations and other third parties. Other issues include the division between ownership and access in the electronic environment, where access controls do not depend on possession of a physical record; the retention and access to patient records for research purposes, the role of the criminal and civil law in relation to misappropriation and misuse of EHRs; and ways in which trust between the doctor and patient are replicated online.

Areas of risk to networked medical records identified by Russell G. Smith include the interception and alteration of confidential communications, online vandalism and terrorism, illegal transfer of funds, unprofessional conduct such as not examining a patient properly or operating in jurisdictions unregistered and the delegation of medical decisionmaking that could also lead to professional liability.[84] If health networking were global, changes to the international registration and special codes of conduct for medical practitioners online would be essential. In principle any cross-jurisdictional control of medical practice would need to take account of Smith's list of risks.

Smith advocates a model that replicates the existing protection mechanisms of the medical profession extended to the international arena, essentially a community of common interest, operating internationally. Legal principles for health networks include applicable rules of conduct and jurisdiction of medical disciplinary bodies; registration of health care providers to be recognised in the jurisdiction in which the patient is physically located at the time the procedure or test takes place; and the health care provider to abide by codes of conduct and rules in the jurisdiction where the patient resides. Security issues include protecting

[84] Russell G. Smith, 'The Regulation of Telemedicine', in *Health Care, Crime and Regulatory Control*, ed. Russell G. Smith, Hawkins Press, Sydney, 1998, pp. 190-203. Smith states that no systematic study of the medico-legal risks associated with the use of telemedicine has been conducted. See his examples of risks, pp. 193-197.

any communication which identifies a health care provider or health care user; access controls and passwords; and the use of digital signatures.[85] The European Union has been a model for the control over medicine beyond national borders well before the advent of the Internet. However, the variations in the way medicine is controlled in different countries, even in the United Kingdom which has had a strong government-medicine alliance, has to be taken into account in a global medical treatment context.

8.5.2 Communities of interest trust model: medical community

The Australian Commonwealth Health Taskforce recommended a 'virtual private network', with in-built security measures to protect privacy in order to overcome the otherwise insecure communications over the Internet.[86] The system would be built on top of a public network as a virtual closed circuit for restricted user groups. A 'closed' intranet system is used in many business contexts, with privacy enhancements including encryption across an unsecured network, access controls, and authentication of the identity of the parties to the transaction. But existing security technologies are not adequate and accessibility over time to encrypted material is uncertain.[87] The need for security in online systems is not unique to the medical context. However, for medical records, additional authentication may be required in relation to each transaction.[88] The 'Good European Health Record Project' links a 'responsible' clinician to a health record. Information does not form part of the health record until a clinician has taken responsibility for entering it.[89] This intentional feature of record making is found in archival science and should be incorporated into all definitions of a health record.

Who is ultimately in control of the EHR is of fundamental importance to its preservation. The regulatory framework that is currently in place can

---

[85] Ibid., p. 199.

[86] Private networks were originally built using owned or leased private lines by firms seeking to establish secure communications amongst a 'closed' group of users. See *A Health Information Network*, Appendix E: Network and Communications Considerations, E9: 'A virtual private network (VPN) is a secure, encrypted connection between two or more points across the Internet'.

[87] *A Health Information Network for Australia*, p. 137, and Appendices E 1 and E 8. The Report indicates here and elsewhere that these 'secure' systems are never really secure.

[88] Ibid., Appendix E 4.

[89] Flinders University, *The Benefits and Difficulties of Introducing a National Approach to Electronic Health Records in Australia,* p. 9.

apply to a web environment only if it is a controlled closed system based on current practice, that is, one in which the EHR is under the control of health professionals. Within the community of interest model the health professional is regulated by a number of rights and duties.[90] In a totally open system the state would be able to gain access to information held in a database, and in a distributed environment individual servers would be subject to attack.[91] A cautious approach that builds on existing regulation would provide greater protection for both the patient and the medical practitioner.

Rights and obligations: ownership and access

The concept of 'custodianship' of the medical record has been proffered as a 'new' approach to ownership and access by health information experts. Custodianship it is claimed would provide control over content and use, with principles based on the rights of the data collector (doctor, medical facility), intellectual rights of the provider and the rights of the community. Multiple 'authors' would have ownership claims which would be unworkable, as their consent would be required each time the record was accessed.[92] A statutory right of access by the patient to his/her medical record is a far cry from the patient owning and controlling the record outright.[93]

If participants are analysed within a recordkeeping framework that differentiates the 'legal authors' from 'writers' then it would not be a question as to gaining consent of every contributor to the health record, but only of the legally responsible person. Using the legal and social relationship model, rights and duties can be identified, with the person who is the subject of the collection as having rights and the 'health service provider' having duties to perform (unless exempt). Other common law

---

[90] Elements of trust (confidentiality, privacy and ethics), identity (ownership and access), and authenticity (evidence) within doctor-patient communications are outlined in Livia Iacovino, Ethical-Legal Frameworks for Recordkeeping: Regulatory Models, Participants and their Rights and Obligations, PhD Thesis, Monash University, Melbourne, 2002, pp. 319-353.

[91] Flinders University, *The Benefits and Difficulties of Introducing a National Approach to Electronic Health Records in Australia,* p. 114. The Flinders Report recommends a closed system together with patient control.

[92] NSW Health Department, *Ethical Management of Health Information, Discussion Paper,* November 1999, Better Health Care Centre, Gladesville, NSW Health Department, 1999, p. 13.

[93] Iacovino, 'Trustworthy Shared Electronic Health Records: Recordkeeping Requirements and Health*Connect.*'

rights and obligations unless extinguished by legislation would continue to be relevant. Privacy should be an element of the relationship, that is protected by a number of means, both legal and social.

Duty of confidentiality and medical privacy online

Confidentiality in the doctor-patient relationship is the major ethical and legal concern when patient information is transmitted electronically and accessed by health providers, hospitals and patients. In the proposed health network for Australia, privacy, confidentiality and security are not defined as legal concepts. The *Health Information Network for Australia* report acknowledges that the unconditional trust placed by the patient in his or her healthcare provider that the information supplied will remain confidential is fundamental in the patient's relationship with the provider.[94] The mechanisms proposed to protect confidentiality include identifiers that are not inextricably linked to a name (patient, health provider or facility) except when needed. However, named identifiers are needed to provide the record with its identity and integrity over time. Therefore an inextricable link between an identifier and the record must also be maintained but protected from inappropriate disclosure.[95]

The piecemeal and inconsistent jurisdictional approach to Australian privacy and health legislative initiatives 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.[96]

8.5.3 Recordkeeping person metadata requirements: doctor-patient online

The EHR has been defined as:

---

[94] *A Health Information Network for Australia*, Appendix F2.3, footnote 87 is the only full reference to Hippocratic ideals and its importance in OECD countries.

[95] Health*Connect, Business Architecture v1.9*, Nov. 2004, Version for Comment, p. 30. Health*Connect* developments point to a national health identifier rather than just a Health*Connect* identifier possibly associated with a personal identifier for all government transactions, thus linking health personal data with an ever widening set of transactions between government (frequently via private deliverers) and the individual.

[96] Moira Paterson and Livia Iacovino, 'Health Privacy: The Draft Australian National Health Privacy Code and the Shared Longitudinal Electronic Health Record', *Health Information Management Journal* vol. 33, no. 1, 2004, pp. 5-11.

> a necessary tool for providing person-centred and continuing health care safely and efficiently in the modern information environment. It is not a stand-alone system in a doctor's surgery or in hospital outpatients; rather, it is a longitudinal collection of information about a person's health that is stored at the point of care, and which may be moved or accessed with the individual's specific consent by health professionals at other sites involved in providing care.[97]

The boundary of the electronic medical record in a networked context is problematic. The definition of a health service in the *Privacy Amendment (Private Sector) Act* 2000 (Cth) provides an activity-based definition that is useful in the electronic context.[98]

In terms of recordkeeping in the web environment the terms used in medical informatics of 'encounters' (transactions) and 'episodes of care' (activity-process), form the basic record unit. A 'business' transactional perspective of patient to doctor, doctor to doctor, and health care facility to doctor is central to a record as a right-duty thing, which is missing in an episodic view alone. How does the EHR operate to authenticate the participants? What metadata is required to prove that a person is a medical doctor and the patient is who he/she claims to be? How are identification and competence persistently linked to the transaction?

Relevant person metadata in the online context for the doctor-patient relationship is summarised in the box that follows. It extends the doctor-patient matrix introduced in Chapter 6 from the viewpoint of the medical provider.

---

[97] Flinders University, *The Benefits and Difficulties of Introducing a National Approach to Electronic Health Records in Australia,* p.1.

[98] *Privacy Act* 1988 (Cth) as amended in 2000, s 6 Interpretation, 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 individual's health; or (ii) to diagnose the individual's illness or disability; or (iii) to treat the individual's illness or disability or suspected illness or disability; or (b) the dispensing on prescription of a drug or medicinal preparation by a pharmacist.

Competent author: doctor/hospital/medical facility. The identity of the facility, location or doctor from where the information has originated: the 'facility identifier' or 'medical provider identifier'(legal author), and the identity of the medical person who has created each piece of information (the 'writer' if not the 'legal author'): the 'medical provider identifier'.
Recipient/addressee: the patient (of action): 'patient identifier'; another doctor/hospital (of communication): 'facility identifier' or 'medical provider identifier'.
Third party/transaction facilitator/ intermediary: authentication authorities such as professional medical bodies; the Health Insurance Commission.
Data subject: the patient.
Service provider: Health Information Network for Australia.
Communications carrier: provider of telecommunications service.
Internet regulators: government authorities; the Commonwealth Government's 'Gatekeeper'.

Authentication framework

How will the trust between the doctor and patient be replicated online? Patient information is protected from disclosure to third parties by medical practitioners via confidentiality in professional codes and the common law but may be disclosed under statutes. Trusted third party channels could include the registration and practice function found in medical boards. Authentication certificates and digital signature verification would logically be issued via this function, depending on the purpose for which it is used.[99] It would only verify that X is a doctor within the competence of that authority, not his/her reliability in any other capacity. In a wider health network this would also be sufficient unless another role was assumed with added responsibilities on the part of the doctor (that is, as a director or registrar). Channels for international trust for a global health network could be provided by countries that cooperate in professional identify-cation. These channels could build on Mutual Recognition Acts which currently require each Australian state to notify other states if a doctor is registered. Each state could issue a 'good standing' certificate for international practice.

[99] Electronic lodgement of Medicare claims adopts digital certificates issued by the Health Insurance Commission to identify doctors under the Gatekeeper program. Stewart Carter, 'Net-based System Paves Way for Use of Digital Medicare Forms', *The Age*, 9 May 2000.

8.5.4 The buyer-seller relationship online

The business to consumer relationship online is an example of a combined legal and self-regulation model. Business to business activity has on the whole more easily adapted to Internet technologies and continued to build on 'closed systems', similar to EDI (Electronic Data Interchange), which operates on exchanges based on prearranged contractual relationships using computer to computer applications in standardised form. Business to consumer transactions over the Internet involve a free form of communication.[100] Legal issues regarding the limits of territorial law are particularly relevant to the buyer-seller if they are transnational transactions.

Regulation of online consumer services

The legal implications of selling goods and services via the Internet include liability for advertising, 'misleading and deceptive conduct', product liability, consumer protection laws (including the law of 'passing off'), and trademarks. It may require defences such as 'due diligence'. Liability may arise under the *Trade Practices Act* 1974 (Cth) s 52 in particular, state and territory fair trading legislation, the laws of negligence and misrepresentation, or breach of contract.[101] However, these laws have limited application outside of Australia. Section 52 covers information on the Internet which originated in Australia, and may be extended to material that originates from elsewhere. Until the courts address the extraterritorial operation of the *Trade Practices Act* 1974 (Cth) s 52 will only apply if the conduct occurred in Australia.[102] Therefore the major problem in the online context is the buyer's rights when goods are bought from outside Australia. However '…provided there is a sufficient jurisdictional nexus between

---

[100] Smith, *Internet Law and Regulation*, Chapter 8.

[101] Willis, 'Intranets and the Law', p. 50. Promoting a product or service is pre-contractual, regardless of whether one is actually selling or providing it online.

[102] Beth Finch, 'Consumer Protection on the Internet', *Going Digital 2000*, *Legal Issues for E-commerce, Software and the Internet*, eds Anne Fitzgerald et al., 2nd edn, Prospect Media, St. Leonards, New South Wales, 2000, p. 263. Consumer protection provisions contained in the *Trade Practices Act* 1974 (Cth) s 51(1) extend to conduct outside of Australia by companies incorporated or carrying on a business in Australia or by Australian citizens or persons ordinarily resident in Australia.

a relevant e-commerce activity and the territory or people of Australia, then the laws of Australia are likely to apply to that activity.'[103]

International context

Major concerns in Internet commerce centre on the ineffectiveness of national laws, as well as international agreements, in particular deceptive practices. When a consumer purchases a commodity a contract is made, which in theory is a free consensual act. The economic power of the supplier does not provide sufficient protection for the buyer, hence the need for consumer law. Each jurisdiction has its own set form of consumer protection legislation. It is usually not possible to override consumer protection legislation via a contract, as this will override any agreed terms in the contract which contravene the rights and protections granted, including such terms as choice of law or jurisdiction.[104]

A 'cyberjurisdiction model' is the emerging international model for consumer protection with rules drawn from UNCITRAL, International Standards Organisation (ISO), World Trade Organization (WTO) and non-government bodies such as Consumer International. The preference has been for the WTO's rules because it has an adjudicatory system. Extralegal redress includes consumer organisations taking action on behalf of consumers against specific traders and international cooperation measures with the OECD.[105] Cases of long distance fraud have occurred using aliases and anonymous sources.[106] Compliance with international regimes still needs resolution.[107]

---

[103] Andrew Sorensen and Matthew Webster, *Trade Practices and the Internet*, Lawbook Co., Pyrmont, NSW, 2003, p. 6. For a detailed analysis of the extraterritorial operation of the *Trade Practices Act* 1974 (Cth) in the context of electronic commerce, see pp. 137-149.

[104] Lars J. Davies, *A Model for Internet Regulation? Constructing a Framework for Regulating Electronic Commerce,* Information Technology Unit, Centre for Commercial Law Studies, Queen Mary and Westfield College, London, 1999, para 3.10-15.

[105] Finch, 'Consumer Protection on the Internet', pp. 277-280. See the UNCITRAL Model Law on Electronic Commerce.

[106] John Goldring, 'Netting the Cybershark: Consumer Protection, Cyberspace, the Nation-State, and Democracy', in *Borders in Cyberspace: Information Policy and the Global Information Infrastructure,* MIT Press, Cambridge, Mass., 1997, pp. 322-354.

[107] Chris Connelly, 'Financial Services Policy - the Interaction of the Privacy and Financial Services Regulatory Systems', in *Papers from The New Australian Privacy Landscape*, Faculty of Law, Continuing Legal Education, The University of New South Wales, 14 March 2001.

8.5.5 Community of interest trust model: commercial community

Rights and obligations: contracting online

The market and the law have pushed for reliability, trust and non-repudiation of Internet commerce which has created new legislation, for example in Australia the *Electronic Transactions Act* 1999 (Cth) and similar legislation internationally. The *Electronic Transactions Act* provides a 'light handed regulatory regime for the use of electronic communications in transactions'.[108] The Act is centred on ensuring that electronic communications have legal validity, in particular, but not exclusively, in contractual circumstances. It provides coverage for identities of parties essential for contract formation, but does not cover specifics, such as terms and conditions.

Contracting online includes evidence of contract formation, offer and acceptance, requirements of writing, and contractual terms. Issues of time and place of contract, that is, when is it reasonable to believe the contract was received, identity of persons contracting, and payment mechanisms are all required. When a buyer-seller contracts online a contract is formed when one party offers to do or supply something on terms which are accepted finally and unequivocally by the other party, and that acceptance is communicated to the person making the offer. Something of value in legal terms must be given to the person making the offer, usually a payment. The record must capture the terms of the contract and evidence that the buyer read the conditions, for example, a web page offer becomes a binding contract on receipt of a user response requesting to purchase a product, unless it is made clear that it is merely an 'invitation to treat'. Signatures to a contract are a formality for certain kinds of contracts only, but identification of the parties to the contract is required. In contract law when a contract is accepted (or it is reasonable to believe that it has been accepted) has to be demonstrated for it to be legally valid. The time of the contract may be when there is a clear acceptance of an offer or it may be when an order is placed (time is also essential to record identity). The place of the contract is relevant where parties have not agreed on which jurisdiction governs, or where there are no applicable international conventions (place is also essential to record identity). The international

[108] Parliament of the Commonwealth of Australia, Senate, *Revised Explanatory Memorandum, Electronic Transactions Bill 1999,* 30 June 1999, General Outline. The *Electronic Transactions Act* 1999 (NSW) and *Electronic Transactions Act* 1999 (Vic) are modelled on the Commonwealth Act.

dimension of online contracts relates to law of applicability and law of jurisdiction.[109]

A contract witnesses many transactions: the agreement, and the terms and conditions that result from the contract process. A contract has been a prescribed legal record. It is both a record as object and as process. The most important question is whether or not a contract was actually formed, and if so, where that contract was formed and when.[110] The necessity to prove an offer and acceptance between unknown parties accentuates the need for a reliable record.

Trade practices and consumer confidence issues are managed by the *Australian Competition and Consumer Commission*. The *Trade Practices Act* 1974 (Cth) Part 5 contains a range of provisions for protecting consumers and corporations as consumers, including s 52 which deals with misleading and deceptive conduct, prohibits conduct which is misleading or deceptive, or which is likely to mislead or deceive. Sellers are required to tell the truth or to refrain from giving an untruthful impression, including disclosure of relevant information. Section 53 prohibits false claims about sponsorship approval, performance characteristics, accessories, and uses of, or benefits from goods and services. These restrictions apply to electronic transactions and electronically supplied information as well as to physical goods and services.[111]

---

[109] The common law is less concerned with the date of receipt of a message than with when the contract takes effect. Davies, *A Model for Internet Regulation? Constructing a Framework for Regulating Electronic Commerce*, Part 3.4 Rules of Contract Formation.

[110] Ibid., para 3.4.8.1. Differences between civil and common law regimes arise. Davis states that 'The approach within the common law is not so much to ask when a message was received as to ask when does it take effect? This is in line with the general focus of the common law on function as opposed to form but this approach can lead to seemingly strange results. An extreme example of the results of this type of approach can be seen in the postal rule which does not depend on the receipt of a message at all for the message to take effect. The rule simply provides that a message takes effect once it has been sent irrespective of actual receipt.'

[111] See also in this chapter, 8.3.6 'Evidence for establishing rights and obligations of Internet participants', in particular electronic transactions legislation which provides some legislative certainty for consumers, such as the identity of seller and location.

8.5.6 Recordkeeping person metadata requirements: buyer-seller online

Person metadata must identify the buyer and seller, unless anonymous transactions are an option. An authentication framework is essential. Trust and identity have to be verified through individual industries. Elements that communicate trust in websites from the point of view of a consumer include factors that produce a sense of trustworthiness and their relative importance. These do not take into account the evidentiary and record-keeping aspects but they contribute to trust when a customer uses an unknown website. Commercial relationships depend on experience and habit over time. Other factors include presentation which includes the reliance on 'form' or the formal characteristics of websites, seals of approval, the interaction of effective navigation, a well-known brand and product fulfilment. Security over personal data should be clearly stated. Effective navigation of the site, particularly for less known brands, and fulfilment of promises, also increases trust.[112] Below is an Internet transaction matrix from the seller's viewpoint.

Competent author: seller (physical or corporate person).
Recipient/addressee: buyer (physical person).
Third party: Australian Competition and Consumer Commission; Australian Securities and Investment Commission (Office of Consumer Protection).
Data subject: buyer; other referenced parties.
Service provider: private or commercial ISP.
Communications carrier: provider of telecommunications service.
Internet regulators: Australian Competition and Consumer Commission; World Trade Organization; OECD; International Standards Organisation; Consumer International.

8.5.7 The citizen-government (state) relationship online

In relation to direct citizen transactions with government, access to the Internet for the whole community is essential. The initial dissemination of government Internet resources has been shifted to take up 'online

[112] Cheskin Research and Studio Archetype/Sapient, *E Commerce Trust Study*, Cheskin Research, Jan. 1999.

business', such as paying bills and fines electronically.[113] Internet-enabled applications for citizens are an emerging international trend which is seen as enhancing democratic processes.[114] The national governments of Canada and Australia and some European countries have moved agency to agency, business to business and customer (citizen) services online and adopted 'portals' to link all transactions of one citizen together, without however having resolved the privacy and ethical aspects adequately. In Canada a federated architecture model includes a public key infrastructure with a secure channel including a 'brand' on the 'window' for the citizens to identify the government agency. 'Portals' have been used as a layer between the original record and the information provided using unique identifiers for each citizen. The benefit of the increased accuracy of data linked by a unique identifier has to be balanced against the risk of increased privacy infringements that may occur when personal information from many sources is electronically linked to one person. Together with the legislative and authentication frameworks, government-citizen transactions are now technologically and legally feasible, but may not always be socially acceptable.[115]

---

[113] Australian governments began using the benefits of service delivery on the Internet in 1997. The Office of Government on Line (OGO) 'Internet 2001' initiatives aimed to make all appropriate government services online by 2001. These included Fedlink 1998 (the federal government's intranet), the Shared Systems Suite and Project Gatekeeper. See Dagmar Parer, 'Integrating Information Resources and Services Through the Intranet', in *Intranets: Problems and Opportunities for Recordkeeping, Proceedings Conducted by the ACT Branch of the Records Management Association of Australia at Parliament House, Canberra, 10-11 March 1999,* ed. Anthony Eccleston, Records Management Association of Australia, ACT Branch, Canberra, 1999, pp. 65-77.

[114] Agneta Ranerup, 'Internet-enabled Applications for Local Government Democratisation: Contradictions of the Swedish Experience', in *Reinventing Government in the Information Age: International Practice in IT-enabled Public Sector Reform*, ed. Richard Heeks, Routledge, London, 1999, pp. 177-193. In relation to the Swedish project analysed in this article, the political and economic context was a central element in how government applied its technology.

[115] Tom Dale, 'Overview of the Policy, Legislative and Regulatory Environment and Issues Facing Electronic Commerce Frameworks and Uptake in Australia', Paper presented at *Doing Business Electronically: Electronic Commerce and Recordkeeping*, Recordkeeping Systems and the Records Continuum Research Group, School of Information Management and Systems, Monash University, Canberra, November 1999.

Regulation of online government services

In Australia the Commonwealth government has been presented as the 'e-government' model for private business to follow.[116] E-government has also been extended to many state governments.[117] The idea of integrated citizen-centred services for Australia federally and at state levels was set in the 1998 government industry statement, *Investing for Growth*.[118] The Commonwealth in this statement made a commitment to an appropriate regulatory framework for electronic commerce so that Commonwealth government information and services could go online by 2001. Many government agencies are engaging in business online. In the Commonwealth sector the National Archives of Australia has in fact used electronic commerce as a means of promoting good recordkeeping.[119]

In *Moving to an Electronic Marketplace* the Commonwealth announced the government's strategy for paying all suppliers to government electronically by the end of 2000 and trading with ninety per cent of suppliers to government electronically by the end of 2001. Essentially this is the government as buyer, the business to business relationship. The 'electronic marketplace' uses 'established trading networks, mainly procurement chains, between component suppliers and manufacturers and between government buyers and suppliers. Through global electronic markets these supply chain networks are inter-related through computing networks such as extranets, the Internet or the World Wide Web.'[120] The government marketplace adopts existing EDI closed systems, but open systems of electronic trading are also encouraged. There is a unique supplier and buyer identification system in place.

---

[116] National Office for the Information Economy, *Government Online: The Commonwealth Government's Strategy,* Department of Communications, Information Technology and the Arts, April 2000.

[117] Jackie Bettington and Sally Algate, 'Convergence and Divergence in the Queensland Public Sector', in *Convergence, Joint National Conference, Conference Proceedings,* the Joint National Conference of the Australian Society of Archivists and the Records Management Association of Australia, 2-5 September 2001, Hobart, pp. 351-376.

[118] Department of Industry, Science and Resources, *Investing for Growth*, December 1997.

[119] Steve Stuckey and Anne Liddell, 'Electronic Business Transactions and Recordkeeping: Serious Concerns - Realistic Responses', *Archives and Manuscripts*, vol. 28, no. 2, Nov. 2000, pp. 92-109.

[120] Office for Government Online, *Moving to an Electronic Marketplace*, Discussion Paper, Department of Communications, Information Technology and the Arts, August 1999, Glossary, p. 26, 'electronic marketplaces'.

8.5.8 Communities of interest trust model: public sector community

Rights and obligations

The citizen-government relationship online still operates within the regulatory framework outlined in Chapter 6. Consumer protection as outlined above for the seller-buyer online is equally relevant to a citizen's rights when transacting with a government department online. The *Electronic Transactions Act* 1999 (Cth) also applies to communications of citizens or corporate bodies with government.

8.5.9 Recordkeeping person metadata requirements: citizen-government (state) relationship online

Government business online in Australia operates on the whole within the one jurisdiction so there are no cross border legal issues involved. However, new third parties in the government-citizen relationship include Internet security providers, for example the Australian Taxation Office provides authentication certification for some government agencies within the Government Public Key Authority (PKA) framework. PKA provides a 'closed system' between the citizen and government.

Person metadata in government online transactions requires additional parties from the PKA authentication framework. Below is a transaction matrix from the public office viewpoint.

Competent author: executive entity (Crown or its representative government agency for example a government business enterprise).
Recipient/addressee: citizen or organisation.
Third party: PKA and Internet security providers.
Data subject: may be recipient.
Service provider: government ISP.
Communications carrier: provider of telecommunications service.
Internet regulators: government authorities; legal and social enforcement mechanisms. Government certification authority, for example Australian Taxation Office.

Legal and social relationships online, as exemplified by examples in this chapter, are currently hampered by inadequate authentication frameworks in relation to the trust elements that communities of common interest have

been able to provide, although business and technological changes have eroded many of the traditional elements. In addition, the retention and preservation over time of record objects with persistent person metadata is still at developmental stages of research, despite a number of excellent recordkeeping metadata schema and templates of record attributes for record identity and integrity. Without the identification and capture of the competencies and moral motives of the recordkeeping participants, their rights and obligations become more difficult to define. Ownership, access, privacy and evidence of records as right-duty things have evolving frameworks in the international context, but are largely enforced by domestic laws, and notions of jurisdiction of sovereign nation states, albeit within international model laws. Notions of materiality-immateriality dichotomies are still evident in laws where frameworks for the paper record as object parallel the electronic version. Legal and social relationships are analytical tools applicable in the online environment for analysing the extent to which current technology provides trust. Social trust continues to play an essential role.