7 RECORDKEEPING REGULATORY MODELS IN THE WEB ENVIRONMENT

Juridical and warrant-based regulatory models for recordkeeping[1] are predicated on regulation pertaining to a specific juridical context or an industry or professional community, which in the online environment depends on a combination of codes of conduct, legal action and technical solutions that have gradually emerged to protect privacy, copyright owners, provide access to users, and to give legal validity to transactions. The records continuum provides a framework in which the Internet legal regulatory models outlined below can be incorporated into recordkeeping models.[2] The OECD and a number of other international bodies have provided voluntary principles on Internet regulation which have guided national approaches.[3] The convergence of law internationally supports the 'pluralisation of collective memory' of records outside of their organisational context in the same way that recordkeeping standards provide a universal language for recordkeeping practice. The necessity for closed networks for particular industries provides validity to communities and professions that operate within their own standards of trust where the legal accountability of the organisation and its corporate memory is the strongest.

---

[1] See Chapter 1.

[2] For example, conceptually an intranet operates at the third dimension, that is the organisational or corporate level, and the Internet at the fourth dimension, that is the institutional or collective level of the records continuum model.

[3] OECD, Directorate for Science, Technology and Industry, Committee for Information, Computer and Communications Policy, *OECD Input to the United Nations Working Group on Internet Governance*, OECD, 2005. For an example of Australian Internet regulatory models see Livia Iacovino, Ethical-Legal Frameworks for Recordkeeping: Regulatory Models, Participants and their Rights and Obligations PhD dissertation, Monash University, Melbourne, 2002, pp. 406-411.

7.1 Regulation of the Internet

Regulation has been defined throughout this book not merely as the law made by parliament and the courts, but also social controls or normative systems other than the law proper. The role of ethics and codes of conduct are of particular relevance to Internet 'self-regulation' models.[4]

Ethicists and jurists over the centuries have failed to achieve a consensus on whether humans act only in their own self-interest and whether benevolent behaviour towards others is 'natural' or learned. It is therefore highly unlikely that a simple answer to these questions applies to human behaviour in the Internet context, where the pressure points for ethical motivation and action may operate differently. The image projected of the Internet through advertising is that of a 'cash nexus' society.[5] However users are too varied to allow for generalisation about their habits. What bonds the users are the same social bonds that tie in other contexts, the same interests and values of communities, in which profit, as Peter Singer would express it, is only one motivation.

For democracy advocates, the Internet was not envisaged as developing into a global universal community or market place, but as a multiplicity of communities that would revitalise civic life, a parallel of universalism and particularism, rather than Marshall McLuhan's picture of a global village with universal moral standards.[6] Law in cyberspace was expected to evolve on the basis of communities with distinct rule sets and self-governance. Both the warrant and juridical models include the notion of self-regulatory communities with quasi-legal systems which conform to an Internet self-regulatory model.

In the short history of the Internet, arguments over its regulation have been both social and legal. Many users of the Internet originally argued against its 'regulation' because they saw its value as a tool for improving

---

[4] Peter Leonard, 'Ethics in Cyberspace', *Internet Law Anthology*, ed. Peter Leonard, Prospect Intelligence Report, Prospect Publishing, Sydney, 1997, pp. 140-141. The Australian government report, *The Global Information Economy: The Way Ahead*, July 1997, advised on a non-regulatory, market-oriented approach which suggested clarifying existing legislation rather than introducing an overarching piece of legislation.

[5] Donna Gibbs, 'Cyberlanguage: What it is and What it does', in *Cyberlines: Languages and Cultures of the Internet,* eds Donna Gibbs and Kerri-Lee Krause, James Nicholas, Melbourne, 2000, p. 18.

[6] Ingrid Volkmer, 'Universalism and Particularism: The Problem of Cultural Sovereignty and Global Information Flow', in *Borders in Cyberspace: Information Policy and the Global Information Infrastructure,* MIT Press, Cambridge, Mass., 1997, pp. 48-83.

equality, and human and political rights.[7] The Open Internet Policy Principles of the Parliamentary Human Rights Foundation promoted the use of the Internet as a means of supporting political freedom, but also recognised the continued existence of national legal systems that are cognisant of international conventions.

> The Internet does not exist in a legal vacuum. For the most part, existing laws can and should regulate conduct on the Internet to the same degree as other forms of conduct. Such laws may differ from country to country, but should conform with the applicable binding human rights obligations contained in the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights and the European Convention on Human Rights.[8]

Self-regulation by cyberspace participants in which the territorial nation state would have restraining powers is one of the earliest notions of Internet regulation. Physical proximity, the legitimacy of law-making within a geographic border and boundaries as signposts that new rules apply when one moves into another space, no longer held sway. An event on the Internet was considered to take place everywhere and nowhere.

Despite the fact that both domestic law and international conventions do apply to the Internet, a popular belief has been that, in fact, it is 'uncontrolled'. Chris Reed, an Internet legal specialist, has termed the notion of the uncontrolled Internet as the 'cyberspace fallacy'. The fallacy derives from the depiction of the Internet as a jurisdiction in which none of the existing rules and regulations apply, a virtual space that expands and contracts as different networks connect and disconnect from each other, and the geographic locations where the activities occur are fortuitous, dictated by the current configuration of the Internet.[9] This outlook can be refuted by the fact that all actors in an Internet transaction have a real-world existence, and are located in one or more legal jurisdictions. The view has been fuelled by the confusion between the applicability of law

---

[7] Parliamentary Human Rights Foundation, *Open Internet Policy Principles of the Parliamentary Human Rights Foundation*, PHRF Conference, Brussels Belgium, 23 November 1996, 'Preamble'.

[8] Ibid.

[9] John Perry Barlow, '"Selling Wine Without Bottles", The Economy of Mind on the Global Net', 1996. In Barlow's thesis cyberspace is a new jurisdiction in which existing rules do not apply. A 'law of cyberspace', or special 'cyberlaw', analogous to the law merchant ('lex mercatoria') was envisaged as a distinctive area of law. See also David R. Johnson and David G. Post, 'The Rise of Law on the Global Network', in *Borders In Cyberspace: Information Policy and the Global Information Infrastructure,* MIT Press, Cambridge, Mass., 1997, pp. 3-47.

and the apparent lack of its enforcement on the Internet, with a conviction that there is an absence of law. In the view of Chris Reed, the Internet rather than being unregulated, is the most heavily regulated place in the world, as all the laws including legal precedents of every country may be in theory relevant.[10]

Technical reasons why the Internet has been difficult to control are due to the technologies that underlie it. It is a decentralised system of many networks based on an open standard Internet protocol which makes it difficult for anyone to block or monitor information originating from many users.[11] Governments, for example Singapore, have been unsuccessful at control over the content distributed on the web, due to regulatory arbitrage, which allows moving an activity to a jurisdiction which is favourable to non-control.[12]

Legal approaches to Internet regulation follow principles that have already been developed to solve disputes when it is unreasonable to apply legal jurisdiction (see below). Proposals for regulation of the Internet have included delegating authority to self-regulatory organisations, establishing net-based law-making institutions or adapting existing ones, for example the World Intellectual Property Organization.[13] The creation of network standards, for example content filters, still leaves a role for the state.[14] The function of international public and private law which requires a choice of forum and choice of law, or alternatively relying on international agreements, have also been relevant to regulating Internet activity.

---

[10] 'Introduction' in Chris Reed, *Internet Law: Text and Materials*, Butterworths, London, 2000.

[11] Sharon Eisner Gillett and Mitchell Kapor, *The Self-Governing Internet: Coordination by Design*. Prepared for Coordination and Administration of the Internet, Workshop, Kennedy School of Government, Harvard University, September 8-10, 1996.

[12] A. Michael Froomkin, 'The Internet as a Source of Regulatory Arbitrage', in *Borders In Cyberspace: Information Policy and the Global Information Infrastructure,* MIT Press, Cambridge, Mass., 1997, pp. 129-163. Arbitrage is defined in the financial context, as the difference in pricing between two counterparties and exploiting the difference for profit, for example, tax havens. The distributed enterprise may use a safe harbour scheme for tax purposes for particular activities. Reed, *Internet Law,* p. 237.

[13] Johnson and Post, 'The Rise of Law on the Global Network', pp. 16 and 24.

[14] Joel R. Reidenberg, 'Governing Networks and Rule-Making in Cyberspace', in *Borders In Cyberspace: Information Policy and the Global Information Infrastructure,* MIT Press, Cambridge, Mass., 1997, p. 96.

7.1.1 Jurisdiction: legal boundaries

Jurisdiction, that is the power of the courts over persons, things and disputes, is geopolitically-based.[15] In the physical world the laws of a particular jurisdiction only have effect within the boundaries of that jurisdiction. Internet transactions are not limited to geographical or political boundaries; national laws apply to some part of their activities. In Internet activity overlaps in national laws are pervasive and encourage law breaking. Even when jurisdiction applies to a matter, a court may not be able to enforce the judgment. Execution of a 'foreign' judgment through judgment recognition depends on recognition treaties, and even then assets (forfeiture) to execute the judgment must be found. The extent to which conventional courts have jurisdiction to adjudicate civil disputes and prosecute crimes on the Internet may require an international criminal court or a private international arbitration panel where the conventional courts cannot operate. Personal jurisdiction, an international law mechanism, requires that a person be present when tried, in particular in criminal trials. Henry Perritt's jurisdiction model for the Internet involves the use of admiralty-maritime law *in rem*, where a wrongdoer does not have to be in the custody of the court to be tried, and compensation for the aggrieved party is pursued through interests held by the wrongdoer. Perritt introduces the concept of a virtual presence in a state.[16] The weaknesses with these early approaches to regulating cyberspace are that they attempt to replicate the existing legal processes.

Where do Internet transactions take place?

On what basis can a national government claim to apply its laws and regulations to Internet activities which originate in a different jurisdiction? How far, if at all, is it possible to resolve the conflict between differing national laws where the only effective means of compliance is to limit information flows across national boundaries?

---

[15] Jurisdiction is also used broadly to include the power of government to legislate in relation to particular persons or circumstances, to adjudicate by subjecting persons to dispute resolutions, and compelling compliance with laws. See Gaye L. Middleton and Jocelyn A. Aboud, 'Jurisdiction 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. 245-246.

[16] 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, pp. 164-202.

Principles have been established via private international law, or conflict of laws, by deciding if a relevant element of a transaction can be localised in the jurisdiction in question. Where did each element of the transaction take place? Chris Reed states:

> The problem with cyberspace is that its constituent elements, the human and corporate actors and the computing and communications equipment through which the transaction is effected, all have a real-world existence and are located in one or more physical world legal jurisdictions. These corporeal elements of cyberspace are sufficient to give national jurisdictions a justification for claiming jurisdiction over, and the applicability of their laws to, an Internet transaction.[17]

'Localisation' in the physical world is defined by where the human actor was situated when the act was performed. For corporate actors in multiple jurisdictions there are various presumptions about place. For example, in contract, place or location of performance is agreed upon as part of the contract. There are exceptions if one of the parties is a consumer. Other factors for localisation include habitual residence of person, principal place of business, place where contract was performed, place where the steps necessary for the conclusion of the contract were taken, and place where an advertisement or invitation to enter into the contract was received. For tortious claims, jurisdiction is where damage occurred.[18]

In diplomatics and rules of evidence, probative value increases with the closeness of the act of documentation to the act itself. Time and place in law vis-à-vis the record is based on the process of executing the act. If physical place is where the transaction occurred, applicable law, according to Chris Reed, is every jurisdiction or else applicable law has no obvious connection with the parties or the substantive transaction.[19] Reed argues

---

[17] Reed, *Internet Law: Text and Materials,* p. 188.

[18] This has been upheld in *Dow Jones Inc. V Gutnick* [2002] HCA 56 10 December 2002. The case decided that the State of Victoria was the place of publication of material that contained defamatory content, even if it was uploaded in the United States. The place of publication is essential to ascertaining where the tort of defamation can be invoked and where the court has jurisdiction. The *Dow Jones Inc. V Gutnick* case indicates that in Australian courts domestic laws are likely to be applied to Internet legal transgressions. In the United States, case law indicates that where a website is outside the territory of a relevant court, carrying on active business with residents of the jurisdiction will attract the jurisdiction of that court. For a discussion on jurisdiction, see Andrew Sorensen and Matthew Webster, *Trade Practices and the Internet*, Lawbook Co., Pyrmont, NSW, 2003, pp. 137-149.

[19] Reed, *Internet Law: Text and Materials,* Chapter 7 Cross-border law and jurisdiction. Local law has been applied successfully in a defamation case in

that localisation is meaningless on the Internet. However, from a recordkeeping view a storage 'space' for the recordkeeping system or where the transactions have been captured whether on a server, hard disk or other storage device, over which an organisation or individual has 'control', is necessary to run a business.[20] Reed is mainly concerned with multiple copies of data on different servers, rather than viewing them from a transactional perspective in which case each 'copy' is the 'original' of the respective records of the organisation.

Enforceability in the Internet environment

The distinction between applicability and enforceability is fundamental to the development of Internet law. Convergence of national laws is one answer to enforceability, but in areas such as free speech it may be

Australia. See *Dow Jones Inc. V Gutnick* [2002] HCA 56 10 December 2002. Although an Australian case has no binding authority on other common law countries, it could be followed in the United Kingdom or other common law countries. The case opens up worldwide liability through foreign legal proceedings. See Andrew P. Sparrow, *The Law of Internet & Mobile Communications: the EU and US Contrasted*, tfm Publishing, Harley, England, 2004, pp.139-140.

[20] Where and when a record resides on a server has been defined in the Australian *Electronic Transactions Act* 1999 (Cth) s 14(3) and (4). 'Where the addressee has given specific directions and the electronic communication is transmitted in accordance with those directions, subclause (3) says that the communication is received when it enters the designated information system. As it is expected that a person who has designated an information system will regularly check that information system for messages, the provision effectively deems the communication to have come to the attention of the addressee as soon as it enters the designated system. In all other cases subclause (4) operates to state that the electronic communication will be received when it comes to the attention of the addressee. *The term "comes to the attention of the addressee" does not mean that a communication must be read by the addressee before it is considered to be received.* An addressee who actually knows, or should reasonably know in the circumstances, of the existence of the communication should be considered to have received the communication. For example, an addressee who is aware that the communication is in their electronic mail "box" but who refuses to read it should be considered to have received the communication' [emphasis added]. Australia, Senate, *Electronic Transactions Bill 1999,* Revised Explanatory Memorandum, 30 June 1999, pp. 39-40.

impossible to reach a consensus. Ultimately enforceability is required if law is to have 'normative force'.[21]

Essentially the unenforceability of the law in the Internet context arises from its trans-jurisdictional nature, that is, all laws applicable to an activity in every jurisdiction may apply in the Internet context. There are two types of enforceability issues: laws and regulations which are, in practice, unenforceable, because the court has no effective jurisdiction over the defendant, generally laws relating to criminal offences, and laws and regulations which are in theory enforceable, but where the cost of the enforcement outweighs the benefits of enforcement, usually private matters.

Industry practice and community expectations have also played a role in regulating cyberspace.[22] For example, to reduce uncertainty with respect to personal jurisdiction, choice of law and venue in civil cases, Perritt recommends the adoption of international arbitration.[23] Communities of suppliers and consumers can adopt their own rules on intellectual property infringement and other matters and apply rules through arbitration machinery agreed upon by the community. Conduct can be judged according to norms developed by the users of the network, and violations are adjudicated by a system of arbitration, with monetary penalties or exclusion from network participation. For example, the terms of service between the service provider and the subscriber are contractual and can operate as an arbitration agreement. The arbitration awards would be enforced worldwide under the New York Convention, or by excluding wrongdoers from the services.[24] Criminal matters require a public

[21] If a law is either unenforceable or unenforced it loses its normative effect as law. Lon Fuller, *The Morality of Law*, revised edn, Yale University Press, New Haven, London, 1969, Chapter 11 as quoted by Reed, p. 252.

[22] Perritt suggests adapting legal 'restatements' of common law, a traditional American Law Institute practice, to cyberspace based on evolving online industry practice. See Perritt, 'Jurisdiction in Cyberspace: the Role of Intermediaries', pp. 190-191.

[23] Regular courts may enforce the arbitration agreement, by 'compelling arbitration'. There has to be an arbitration agreement in which rules of evidence are written into the agreement, cost allocation, and reference to rules of procedure issued by bodies sponsoring the arbitration, such as United Nations Commission on International Trade Law (UNCITRAL). General commercial law rather than substantive law may be applied. 'Arbitration is a dispute resolution process in which a binding decision is made by one or more private individuals under an agreement entered into by the disputants'. Perritt, 'Jurisdiction in Cyberspace: the Role of Intermediaries', p. 185.

[24] Ibid., pp. 184-188.

international court. The current International Court of Justice only handles disputes between nations. An international criminal court may be an avenue, but has many stumbling blocks.[25] The arbitration approach to jurisdiction in cyberspace is similar to the juridical model, that is, it is based on a set of rules sanctioned and enforced by a community with common interests.

International law includes private and public international law (also referred to as transnational law). There are no real sanctions for breaches of public international law. In fact legal positivists deny that international law has the status of law, although it has moral and political force. In most countries it needs to be incorporated into local law. Private international law is part of the local law, and includes whether any state has legal jurisdiction between citizens or between citizens and states; whether a state can enforce a judicial determination (recognition and enforcement) and the body of rules that will be applied to resolve any issues that arise (choice of law). Private international law is relevant to the Internet, and civil remedies are easier to enforce as most Western legal systems accept legal orders of foreign countries that have jurisdiction, although approaches to recognition and enforcement of foreign judgments differ from country to country. A court has jurisdiction even if a person is only briefly in its territory. However apart from commercial-contractual obligations, other areas such as product liability are difficult to enforce if a country does not have similar laws. Generally no state can exercise its own laws in another state without the agreement of the other state. Extradition, when one state requests another to apprehend and surrender to it a person, is complex, therefore activities online that are deemed criminal need to be assessed by domestic laws of all states.[26] Rather than broadening the role of international courts, new laws, in particular in the copyright area, have gone ahead.

Self-regulation schemes, particularly for private rights, already exist for privacy and other rights. They are backed by sanctions for non-compliance, for example loss of the 'seal' from the 'group' or schemes

---

[25] An international criminal court under the United Nations came into force on 1 July 2002. Its focus is war crimes, and therefore only computer crimes of serious magnitude are likely to be included. The United States has been one of the countries that dragged its feet on establishing such a court, wanting immunity from prosecution for its military from any international criminal court.

[26] 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. 334-354.

linked to legislation. Consortia of Internet Service Providers and Internet Watch Groups use the 'seal of approval' approach. Effective enforcement involves self-regulation coupled with alternative enforcement resolution.[27]

The trend for enforcement in the Internet environment is being resolved by identifying infringements that are likely to arise in any jurisdiction, and applying local laws. This approach is slowing building a common body of Internet law.[28]

7.1.2 Convergence of national law

> In the longer term, the Internet and the commercial and non-commercial activities carried out by means of it will impose substantial pressure on national legislators to eradicate the differences between their own laws and those of other states ...[29]

A national government can try to enforce its laws on Internet activities emanating from foreign jurisdictions in its own country, but enforcement in another country is another matter. Governments may apply the principles of 'comity' which require that a state should not claim to apply its legislation to persons within another state unless it is reasonable to do so. Legislators attempt to maintain comity by applying their laws only to activities undertaken within the state. It is a form of localisation, but uses different triggers. Rather than localising Internet activities, comity is maintained by accepting 'country of origin' regulation, coupled with an appropriate degree of harmonisation or convergence of national laws.[30]

Home country or 'country of origin' regulation, adopted by the European Union, is the only regulatory model so far attempted that Reed believes is capable of resolving the conflicts between multifarious and overlapping claims by national jurisdictions to regulate Internet activities.[31]

---

[27] Reed, *Internet Law: Text and Materials,* pp. 267-268.

[28] Reidenberg, 'Governing Networks and Rule-Making in Cyberspace', p. 96.

[29] Reed, *Internet Law: Text and Materials,* p. 271.

[30] Ibid., p. 204. Reed's examples are taken from heavily regulated activities such as banking and finance. Having a permanent establishment in the relevant jurisdiction is the primary trigger for the application of financial services regulation, and for income tax liability. A website hosted on a server where the server is a business asset is treated as part of the enterprise (if the website were hosted by an independent ISP there would be no permanent establishment). The concept of a permanent establishment has to be modified radically, as many websites are not located in the jurisdictions where they do business.

[31] See Stephen Weatherill, 'The Regulation of E-Commerce under EC Law: the Distribution of Competence between Home States and Host States as a Basis

By mutual agreement two states, or a group of states collectively, provide that activities of an organisation which is established and regulated in one state (the home state) may be carried out in another (the host state) without any requirement for prior authorisation from or supervision by an appropriate regulatory body in the host state. The basis of this agreement is an assessment by all participating states that the others operate systems of authorisation and/or supervision which are adequate to achieve the aims of the home state's regulatory system. The laws of the host state will apply to the appropriate aspects of individual transactions undertaken in the state, for example the law of contract.[32] The essence of country of origin regulation is the acceptance by the host country that the home country provides an adequate and broadly equivalent level of regulatory oversight.[33] Online actors can be regulated in their home country by the mechanism of an international convention, implemented into national law by the states who are parties to the convention.

In conclusion, the best means for achieving global regulation is through the convergence of national laws, which conform to international laws, conventions, treaties or model laws.[34] There are two different methods for converging law. One involves an international treaty that binds parties to certain matters that must be included in new laws or require laws to be

for Managing the Internal Market', in *E-commerce Law: National and Transnational Topics and Perspectives*, eds Henk Snijders and Stephen Weatherill, Kluwer Law International, The Hague, London, New York, 2003, pp. 9-25. See also Sparrow, *The Law of Internet & Mobile Communications: the EU and US Contrasted*, pp. 71-72.

[32] Reed, *Internet Law: Text and Materials,* pp. 217-218. An example of an approximation style national scheme is the European Union's 'single passport' for banking services. A credit institution established in, and regulated by one country, is free to provide banking services in all other countries. There are comparable schemes for financial, insurance and electronic signature services.

[33] Ibid., p. 221. Home and host country regulation does not have to be the same, just broadly equivalent.

[34] For example, the international legal principle of *jus cogens* requires a general universal law that has to be adhered to before an international treaty can pass, that is, an international consensus on an area must apply universally. Behaviour that is universally unacceptable, for example, genocide, provides the parameter for deciding on priorities in areas to regulate. Enforcement is through the extension of the principles of territoriality, strengthening international criminal law, and implementation nationally of agreed principles. Viktor Mayer-Schönberger and Teree E. Foster, 'A Regulatory Web: Free Speech and the Global Information Infrastructure', in *Borders In Cyberspace: Information Policy and the Global Information Infrastructure,* MIT Press, Cambridge, Mass., 1997, pp. 244-247.

amended. International conventions already exist for intellectual property, privacy and commercial law. The 'convergence' of law in areas of universal concern on the Internet, such as pornography and privacy, provide a working model. The European Union data protection schemes are based on national or 'home country' regulation, that is, each country has to have an adequate level of protection, and is also applied to non-European Union countries that trade with the European Union. Home country regulation is far less workable where there are conflicts between national laws.[35] The alternative approach is the 'model law' which is based on existing rules together with new rules added by experts, and approved by representative governments. They are sufficiently similar to provide uniform standards of conduct, with local variations if needed, for example the United Nations Commission on International Trade Law (UNCITRAL), which is the basis of national electronic transactions legislation.[36] The 'model law' has been the trend followed in major areas of concern such as electronic commerce. National jurisdiction is still meaningful, but global approaches provide an essential umbrella for areas of universal concern.

7.1.3 Recordkeeping and web 'business' transactions

Recordkeeping functionality in web-based systems has been slow to emerge.[37] The current web context is characterised by the 'one-stop shop' websites, for example portals acting as a single entry into the Internet or into an intranet. 'Intranets' and 'extranets' are used by businesses to

---

[35] Publishing information that contravenes the laws of foreign countries is possible, if the website is hosted elsewhere. Reed, *Internet Law: Text and Materials,* pp. 231-232. However, *Dow Jones Inc. V Gutnick* would now have to be taken into account.

[36] Goldring, 'Netting the Cybershark', pp. 340-351.

[37] The National Archives, United Kingdom, *Management of Electronic Records on Websites and Intranets: an ERM Toolkit*, Dec. 2001; National Archives of Australia, *Policy and Guidelines for Keeping Records of Web-based Activity in the Commonwealth Government*, revised January 2001. Initial studies on websites found that there were no provisions to capture web records into a recordkeeping system. See Richard Barry, 'Factoring Web Technologies into the Knowledge Management Equation ... for the Record', 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. 10.

demarcate the use of the Internet for specific types of functions, often on industry or 'communities of common interest' lines, for example banking, retail, and health.[38] Intranets are also used within an organisation as a vehicle dedicated to carrying out core business including recordkeeping. Electronic service delivery online includes government business to business activity, and an increasing requirement to identify website owners and consumers for business transactions.

While security is a continuing thorn in the side for all businesses using the web, recordkeeping software now exists that creates an enduring audit trail of each customer's web session exactly as the user saw it, and can be 'archived' as a record.[39] However as a record must be intentionally created for a 'business' purpose, and form part of a business process, only transactions that are needed for business should be captured. The process is essentially no different from the kinds of recordkeeping metadata that must be captured to create a reliable record. The record has to identify the parties to the transaction, and capture other metadata on time and place, in order to resolve any dispute about what someone saw on the website when the transaction occurred. This includes evidence of what a consumer saw in cases of misleading advertising and other consumer law issues. Therefore evidence of action has to be incorporated into website functionality, or specifically the intranet has to operate as part of the recordkeeping system of an organisation.

What legal liabilities ensue from the nature of recordkeeping related to doing business on the Internet? Legislation to facilitate the use of the web

---

[38] 'The intranet is the use of internet technologies within an agency deployed on an internal network based on open WWW technologies'. The intranet and the Internet can use the same server. By selective extension an intranet becomes an extranet. Extranets are external intranets that allow an organisation to permit selected customers or suppliers to securely connect via the web to carry out electronic commerce or other transactions. However public access websites are also used for business transactions, so the distinction between extranets and the Internet is blurred. See Barry, 'Factoring Web Technologies into the Knowledge Management Equation ... for the Record', pp. 9-12.

[39] 'Webcapture' is a software product which creates an enduring audit trail of each customer's web session, 'exactly as the user saw it', for dispute resolution purposes. This still allows the customisation of the page for each user. It has potential for recordkeeping online if linked to appropriate metadata. David Braue, 'Seeing Is Believing for Online Dealers,' *The Age*, 2 March 2001. Vignette is the distributor of 'Webcapture'. See also the Indiana University Electronic Records Project, Phase II, 2000-2002, which addresses the capture of electronic records from transaction-based systems by using portal technology and a workflow engine.

for commerce so that electronic transactions are legally acceptable, supports the creation and capture of records. For example, in the *Revised Explanatory Memorandum* to the Australian federal Electronic Transactions Bill 1999 (Cth) an 'electronic communication' is defined as 'a communication of information by means of guided and/or unguided electromagnetic energy. The term "communication" should also be interpreted broadly. Information that is recorded, stored or retained in an electronic form but is not transmitted immediately after being created is intended to fall within the scope of an "electronic communication"'.[40] Therefore an intention to transmit the communication makes it a valid communication for the purposes of the Act. The definition below of transaction includes non-commercial ones and its broad meaning would capture all kinds of communication over the Internet.

> 'Transaction' is defined to include transactions of a non-commercial nature. This term is intended to be read in its broadest sense of doing something, whether it be conducting or negotiating a business deal or simply providing information or a statement. It should not be read narrowly to confine it to contractual or commercial relationships. Nor is it limited to the actual transmission of the information. The purpose of this definition is to clearly include within the meaning of transactions any transactions with or by the government. For example, it includes activities of government agencies in their role as service providers and it includes instances where citizens furnish information to a government agency. This definition is intended to remove any doubt about the broad meaning of the word and is not intended to limit the existing breadth of the legal meaning of 'transaction'.[41]

The relevance of consent to electronic communications is expressed as:

> 'Consent' includes consent that can reasonably be inferred from the conduct of the person concerned. This term is used in clauses 9, 10 and 11 in provisions that state a person must consent to receiving information in the form of an electronic communication. While consent would clearly be demonstrated by a person's express statement of consent, the purpose of this definition is to ensure that express consent is not required in every case and that *consent can be inferred from, for example, a history of transactions or previous dealings*. However, when determining whether consent can be inferred from a person's conduct it will be necessary to look at the circumstances of the electronic communication, including the express statements of the person.[42]

---

[40] *Electronic Transactions Bill 1999,* Revised Explanatory Memorandum, p. 21.

[41] Ibid., p. 23. The term 'transaction' as defined in cl 5 of the Electronic Transactions Bill 1999.

[42] Ibid., p. 20. [Emphasis added]

As established in previous chapters, intention and consent are also important to legal liability and to moral responsibility. The *Electronic Transactions Act* 1999 (Cth) requires evidence of implied consent to continuous dealings and therefore supports capturing communications systematically in recordkeeping systems, not just as one-off unrelated communications. Systematic capture of communications is an essential recordkeeping function.

Controls over domain names also have recordkeeping implications as they affect identity ('owners' of a website), and their reputation.[43] The reliability and the authenticity of the website creators are essential to the credibility of the records. Domain names provide a provenancial source, thus registries of domain names, owners, registration details are record-keeping metadata essential to networked records.[44]

A record in the Internet context is more than just any kind of electronic information or data, with the notion of 'communication' over the Internet as pivotal to the recognition of record transactionality. The adoption of the terms 'electronic communication' (from information technology) and 'transaction' (from business) in Australian electronic commerce legislation are examples of this change.

---

[43] No one has been regarded as the 'owner' of the Internet, however the management of domain names and a number of other areas that originated in the United States are now assigned by the Internet Corporation for Assigned Names and Numbers, a non-profit public benefit corporation. It is responsible for both formal and informal procedures, coordinates domain-name assignments, Internet Protocol addresses, and root server management. These areas do impinge on legal regulation in particular the control over domain names, trademark and 'brand' connections. Milton Mueller, Commentary, 'ICANN and Internet Regulation', in *Communications of the ACM*, vol. 42, no. 6, June 1999, pp. 41-43.

[44] The authenticity of actual sites is an issue that has been tackled by the Australian government. Paul Twomey, 'The Information Economy and Electronic Recordkeeping: An Australian Perspective', in *Archives at Risk: Accountability, Vulnerability and Credibility*, Australian Society of Archivists Conference Proceedings, 29-31 July 1999, Brisbane, ASA Inc., Canberra 2002, pp. 33-36.

7.2 Ownership, privacy, access, evidence and recordkeeping on the web

Different countries have taken diverse paths in relation to regulating the Internet.[45] Some countries have passed technology-specific legislation, for example United States digital signature legislation, while other countries have technology-neutral law or 'electronic equivalencies', for example Australian electronic commerce and copyright law, so that both the tangible old world product continues to be protected as well as the new one. Changes in evidence law have been supportive of recordkeeping concepts and these have been endorsed in the electronic commerce frameworks. Electronic commerce, privacy and intellectual property legislation are also examples of where there are existing global frameworks that accommodate divergences in national jurisdictions.

7.2.1 Ownership and web 'business' transactions

There are a number of approaches that can be taken to the issue of ownership of records in the web environment. These include replacing property concepts with process or provenance definitions for establishing ownership over records, as discussed in Chapter 5. Other approaches are analysed below.

Personal property law

The legal concepts of ownership, previously tied to the material or tangible form of a record, is a major legal issue on the Internet, due to the legal classification of personal property law on the basis of a corporeal-incorporeal dichotomy.[46] Some property lawyers suggest replacing the term 'record', which has been aligned to its physical container or medium such as paper, with electronic 'information', as a more appropriate means of controlling a thing that is intangible. Case law has been reluctant to treat

[45] Chapter 5 covered the issues of ownership, privacy, access and evidence of records and the areas of law which are used to claim ownership or invoked when proprietary information has been 'stolen', sold, or copied. This chapter analyses some of the ways that proprietary information, privacy, access and evidence are, or could be, protected in records in the Internet environment.

[46] With some exceptions, property concepts such as possession, custody and control have applied only to a tangible material object. See Simon Fisher, 'The Archival Enterprise, Public Archival Institutions and the Impact of Private Law', *Archives and Manuscripts*, vol. 26, no. 2, Nov. 1998, p. 354.

information as property, for example when electronic data is deleted or modified it has not been considered as theft or damage to property. Instead unauthorised access must be proven.[47]

Chris Reed presents a picture of 'dematerialised' communications which never produce physical objects.[48] He argues that each computer by passing on copies of documents makes traditional legal distinctions of originals and copies meaningless. However, from an archival science perspective, it can also be argued that like paper records, 'copies' of a digital document may be in multiple locations. It is the document's insertion into the recordkeeping system or linked by an 'archival bond' to related documents that makes it a record. Within a recordkeeping perspective of legal and social relationships it has been argued that the record is a 'right-duty' thing as relationship which is both an object and the result of a process, which transcends issues of physicality. In a number of evidence laws, a 'document' has been extended to include all forms of recorded information[49] that eliminates the materiality-immateriality distinction.

The law of obligations

As property is a legal relationship, the law of obligations would appear to provide another way of protecting property in electronic networked records. Instead of a relationship between a person and an object (the record) that exists in personal property law, the relationship is between two persons and their duties and rights in respect of ownership. This model has merit in the Internet world where legal and social relationships are being

---

[47] Reed, *Internet Law: Text and Materials,* p. 149, footnote 8, refers to *Cox v Riley* (1986) 83 Cr App Rep 54 in which the defendant was convicted of criminal damage when he deleted computer programs stored on a magnetic tape; the damage was to the storage medium. The case was considered conceptually problematic and was later overturned by the *Computer Misuse Act* 1990 (UK) s 3, by substituting a new offence of 'unauthorised access' to a computer with intent to modify its contents, and thus avoiding property terms.

[48] Ibid., p. 148. See also Thomas Hoeren, 'Electronic Commerce and Law: Some Fragmentary Thoughts on the Future of Internet Regulation from a German Perspective', in *Legal Aspects of Globalization: Conflict of Laws, Internet, Capital Markets and Insolvency in a Global Economy*, eds Jürgen Basedow and Toshiyuki Kono, Kluwer Law International, The Hague, London, Boston, 2000, pp. 35-47.

[49] See Chapter 2, 'Rules of Evidence and Trustworthy Records' and the definitions of documents in the Australian *Evidence Act* 1995 (Cth), Dictionary, Part 1, as 'any record of information'; the *Acts Interpretation Act* 1901 (Cth) s 25 and the *Archives Act* 1983 (Cth) s 3(1).

redefined. As the law of obligations is a private law concept, it applies to private transactions which are the dominant form of interchange on the Internet. It can be developed further in the online context if rights and duties pertaining to ownership are tied to specific legal and social relationships.[50]

Reconceptualisation of property: intention, control and ownership

Fisher provides an exposé of the property term 'possession' as interpreted via case law.[51] It has two dimensions: 'intent' (legal possession) and 'control' (actual/de facto possession), which are used to identify who has possession and how it is realised in practice. These understandings of possession are concepts that can apply in relation to 'control' over networked electronic records through the notion of the 'intent to possess' as control. However, Fisher also points to the fact that possession and ownership do not change between entities that are the same legal person, for example in a Westminster system the archival authority and other government agencies are the same legal person, that is, the Crown. An archival authority cannot gain possession, only custody of a government agency's records, unless possession is split along the lines of 'intent' and 'control without immediate physical possession'. Custody therefore remains an important property tool for archival preservation.

Ownership is not only based on physical possession. An alternative concept associated with 'custody' of records, encompasses rights over records by a third party, the records however remaining in the physical possession of the creator. This is recognised in relation to access to records under Freedom of Information laws when the government outsources particular activities; the records are considered to be in the possession of the government agency, even if physically with the outsourcer. It is termed 'constructive possession'.[52] A contract could also assign ownership rights

---

[50] See Chapter 8, 'Legal and social relationships online: the medical, consumer and government context'.

[51] Chapter 5 on legal and actual possession introduced the notion of possession without physical possession and rights of possession as intention and 'control' which are particularly appropriate in the digital environment. See Fisher, 'The Archival Enterprise', pp. 332-333 and Albert Kocourek, *Jural Relations*, 2nd edn, The Bobbs-Merrill Company, Indianapolis, 1928, p. 372.

[52] W.B. Lane, 'Government Decision Making-Freedom of Information and Judicial Review: Accessing Government Information', in *Government Law and Policy, Commercial Aspects,* ed. Bryan Horrigan, The Federation Press, Leichhardt, NSW, 1998, p. 121 and Madeline Campbell, 'FOI Access to

in records held by an Internet service provider or computer host to another party.

Property law could remain a powerful control tool over recordkeeping in the Internet context if it could divest itself of the materiality-immateriality dichotomy. The distinction is really a red herring. As Frank Upward has suggested, what really matters is the 'intent' to have a recordkeeping system (Fisher's 'intent to possess'), while the logical design of the system and its implementation (physical) is 'control'. Materiality remains within the physical implementation tasks, but 'control' resides with the 'intent' taken account of in the design of the system.[53] Intent and control are inextricably connected. The disappearance of recordkeeping containers which stem from a physical sense of object is similar to computer 'objects'. However there are still electronic containers in the form of electronic documents. A digital object can have layers of contextual data that include authorship and access rights that can be redacted for different users, and it is independent of the media on which it is stored. In fact the core object and its related parts that give it meaning are logically connected by software, thus it is a 'thing-object as relationship'.

Metadata-encapsulated objects have physicality; they should be able to be 'bailed' or controlled through constructive possession. For example, 'control' is adopted in the *State Records Act* 1998 (NSW) s 6 in relation to the record owner (the state) and the person in possession of the record. The provision enacts that a person has 'control' of a record if she/he has possession or custody of it, whether directly or personally, or indirectly or remotely through another person, thus resorting to property concepts that may involve either bailment or constructive possession.[54] The provision retains property concepts because possession is important to control.

Control is really intent to possess. Archival institutions could be implementation sites, and claim physical possession. In the 'virtual

Electronic Records', in *Playing for Keeps,* ed. Stephen Yorke, Australian Archives, Canberra, 1995, p. 191. Constructive possession within Freedom of Information legislation has been a difficult legal argument to adopt in terms of ownership.

[53] These ideas grew out of a discussion on the materiality-immateriality dichotomy with my Monash colleague, Frank Upward, in 1998-99, an expert on the application of postmodernist thought to recordkeeping concepts and practices. The ideas have potential for further development. Upward's argument is that the physical recordkeeping containers now need to be viewed logically and that the operational sites for recordkeeping are the new physicality. The immateriality-materiality division has been reshuffled. In his postmodern form of phrasing, the old duality is replaced by a variable dualism.

[54] Fisher, 'The Archival Enterprise', pp. 343-344.

archives' location is still relevant. Storage of and responsibility for control over the records over time, and their ownership, have to be attributed and managed.

A separation of de facto possession from legal possession is endorsed in the International Records Management Standard. It supports the arrangement of records that are physically stored in one location but owned by another person or entity.

> Records systems should be capable of supporting alternative options for the location of records. In some cases, where the legal and regulatory environment allows this, records may be physically stored with one organization, but the responsibility and management control reside with either the creating organization or another appropriate authority. Such arrangements, *distinguishing between storage, ownership and responsibility for records, are particularly relevant for records in electronic records systems.* Variations in these arrangements may occur at any time in the systems' existence and any changes to these arrangements should be traceable and documented.[55]

Distributed custody or distributed management provides for electronic records that may never be physically transferred to an archival agency even if they are under the legal custody of the archives.

Despite Fisher's elucidation of the division of property into intent to control as a form of possession, property law still distinguishes ownership and control. Another approach has been to simply replace the concept of ownership associated with a document as object with 'control' or 'custodianship' of networked records. Some medical information managers propose custodianship as a means of control over content and use of personal medical information, with access principles based on rights of the data collector, intellectual rights of the provider and rights of the general community to the patient information.[56]

Given property law's entrenchment in material and immaterial distinctions, it is being jettisoned for rights of access and control by different parties to networked records. Fisher's 'intent' (legal possession) and 'control' (actual/de facto possession) are not distinguished. The law of obligations rather than common law property concepts have been adopted to some extent by the move to access rights of different parties. The need to distinguish between ownership, access and storage - where records are held and who owns them - is essential to web transactions.

---

[55] ISO, *International Records Management Standard,* ISO 15489-1, section 8.3.4, 'Distributed Management'. [Emphasis added.]

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

Common law rights and property

Simon Fisher has suggested that common law rights found in torts, equity and contract may protect 'intangible property', but are largely untested. The use of the tort of conversion as it applies to rights over incorporeal property, such as money, may apply to electronic data, and the tort of 'spoliation of evidence' that is, seeking damages for intentionally destroying records, could apply to records in any form.[57] Trespass also has application to interfering with electronic information.[58]

7.2.2 Intellectual property and web 'business' transactions

Intangible personal property, protected through intellectual property, in particular copyright, patents and trademarks, has been the major developmental area in Internet regulation. Copyright, in particular, because of its obvious connection to the content on the Internet, may provide a

---

[57] Danuta Mendelson, *Torts,* 3rd edn, Butterworths Casebook Companions, Butterworths, Sydney, 2002, pp. 118-119. Mendelson's explanation of 'spoliation of evidence' is as follows: '… The Privy Council in *The Ophelia* [1916] 2 AC 206 extended the operation of the [spoliation] maxim to the negligent destruction of evidence. The maxim has been recognised in Australia (*Ford v Andrews* (1916) 21 CLR 317 at 324; *McHale v Watson* (1964) 111 CLR 384 at 398). In the United States, *Smith v Superior Court* 198 Cal Rptr (Ct App 1984) was the first to establish an independent tort of spoliation of evidence, which safeguards the interest of the parties to a civil litigation in preservation of evidentiary material against an unreasonable interference with it. Although the majority of cases so far have involved spoliation of objects, the advent of shredding machines, and, more recently, the widespread use of electronic records and their potential for destruction of documents that may be vital to the outcome of civil litigation should help the recognition of this cause of action in Australia.' See also US-InterPARES Project, *Findings on the Preservation of Authentic Electronic Records*, Final Report to the National Historical Publications and Records Commission, 2002, pp. 87-88.

[58] Trespass to goods is the unjustified interference with or denial of the owner's right to possession of the goods. Chris Reed interprets trespass to apply only to the server (= goods) on which the website is stored, as the website is 'intangible'. Reed, *Internet Law: Text and Materials,* pp. 69-70. In footnote 5, p. 69 he refers to an alternative view of trespass based on theories of property which include unauthorised access to the website. Trespass only provides a remedy against interference with goods or land which adversely affect the plaintiff's right of possession. If trespass is developed to encompass the transient interference with the land or goods involved in accessing a website, the person making the link is not trespassing, only the viewer.

preferable legal means of ownership of electronic records rather than concepts of personal property already discussed.[59] For recordkeeping professionals it is more likely that evidence and contract law will remain the cornerstone of the legal issues relating to transactions on the Internet, but copyright law is also increasingly relevant (see below).

Intellectual property, in the electronic information industry has included databases, individual items in a database, computer software and even inventive hardware.[60] An electronic recordkeeping system is likely to be classed as a database. However, intellectual property presents difficulties as rights prevent others from performing certain acts in respect of the protected 'work'. Copyright protects the form of expression, not the ideas or the data in the work. The form and the expression are no longer united in electronic products. The 'rights' rather than the property are 'intangible' and the item protected needs to have a 'material form', such as a film, or a literary work. The text of a web page is protected in different 'forms', as a literary work, graphic images as artistic work, sound and video as sound recording and as film, and the whole as a compilation (a literary work).[61] Despite difficulties with enforcement, there is no question that copyright does subsist in transactions on the Internet.[62]

With Internet access, records, like other information resources, are likely to be accessible directly from the creating agencies or archival authorities by remote users. 'Transmission', 'copying', and 'reproduction' occur simultaneously (which are rights of the copyright owner), when online public access is available. This means that copyright law applies to access where it did not for its analogue counterpart. Access to records that may have been free in the paper world when access and copying were separate activities, now has to be paid for as part of copyright permissions.

'Internet' copyright law: the international context

Intellectual property has an existing international framework which provides protection outside the country of creation of a 'work' at least for the signatories of the *Berne Copyright Convention* to which many

---

[59] Graham J.H. Smith et al. (eds), *Internet Law and Regulation: A Specially Commissioned Report*, F.T. Law & Tax, London, 1996, p. 13.

[60] Charles Oppenheim, *The Legal and Regulatory Environment for Electronic Information,* 2nd edn, Infonortics Ltd, Calne, 1995, p. 3.

[61] Reed, *Internet Law: Text and Materials* p. 73.

[62] Edward A. Cavazos and Gavino Morin, in *Cyberspace and the Law,* MIT Press, Cambridge, Mass., London, 1994, p. 56.

countries belong.[63] It is an international right and therefore of particular importance to online copyright protection. The treaties between member countries usually provide national protection which means that the law of the country where the work is used is applied.[64] The international treaties only cover minimum standards, and domestic copyright law differs substantially from country to country.[65]

However, with the Internet, there has been uncertainty about where a work is 'used'. It could be where it is uploaded onto a website, or where it is downloaded, or perhaps in other countries along the way. As recent court cases suggest, the question of which country has jurisdiction over the Internet is a source of debate around the world. The relationship between the location where the work was originally posted and the place where the infringement has occurred is relevant. Jurisdiction is decided on the rules of conflicts of laws in each country (see jurisdiction above). Because of the diversity of copyright schemes there may be difficulty in a consensus on the model to follow in a single international copyright law.[66]

The Internet has brought together both restrictive and permissive copyright regimes, that is, those that protect and control the distribution of intellectual products and those that consider it inefficient to do so.

---

[63] One hundred and sixty states are parties to the *Berne Copyright Convention* as of April 2005. In 1994 the Berne Convention was incorporated into a major international treaty as TRIPS (Trade Related Aspects of Intellectual Property), which is administered by the World Trade Organization and has mechanisms for breaches via trade sanctions. See Brian Fitzgerald, 'International Initiatives Concerning Copyright in the Digital Era', 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. 90.

[64] If a copy is made of an article published by an American author in Canada, then Canadian copyright law applies. It is possible to have a treaty that applies protection one would receive in one's home country. This is the principle of reciprocity. Ibid., pp. 87-89. Trade agreements also affect domestic copyright law, for example the Australia/US Free Trade Agreement (AUSFTA). See Australian Copyright Council, *Access to Copyright Material in Australia and the US,* Information Sheet G087v01, September 2004.

[65] Jane C. Ginsburg, 'Putting Cars on the "Information Superhighway": Authors, Exploiters and Copyright in Cyberspace', in F. Hugenholz, *The Future of Copyright in a Digital Environment,* Information Law Series, no. 4, The Hague, Kluwer Law International, 1996, pp. 189-220.

[66] 'Editorial', *The Copyright & New Media Law Newsletter: For Libraries, Archives & Museums,* vol. 5, issue 1, 2001. See also Masato Dogauchi, 'Law Applicable to Torts and Copyright Infringement through the Internet', in *Legal Aspects of Globalization,* pp. 49-65, in which he suggests that a single set of copyright laws is difficult but should be pursued through the WTO.

Localisation of piracy in information products has moved to anywhere in the world. Bringing more countries into an international regime is posited as a solution.[67] The 1996 World Intellectual Property Organization (WIPO) treaties referred to as the 'internet treaties' were precipitated by issues of enforcing copyright law in relation to content communicated via the web.[68] They required countries adhering to the Berne Convention to amend their copyright legislation to conform with the articles of the treaties.[69] The most relevant changes in the treaties have related to Article 8, referred to as the right of 'making available to the public' which specifically covers uses of copyright in online services and Articles 11 and 12 that deal with technological circumvention obligations. The articles provide an example of where the Internet and other communication technologies have called for a new approach to copyright law.

The disagreements among the Berne convention countries over the 1996 WIPO *Treaty on Intellectual Property in respect of Databases* is a recent example of the difficulties of international agreement on intellectual property.[70] One of the controversial issues here was the new *sui generic* right for databases as a whole to be a separate category, apart from protection for individual content such as an image, which would prevent the use of a substantial part of the database for fifteen years, renewable when significantly updated. In theory a database would be protected forever. Compilations of data presently receive protection under copyright in the selection and arrangement of data. The data itself has generally not

---

[67] Dan L. Burk, 'The Market for Digital Piracy', in *Borders in Cyberspace: Information Policy and the Global Information Infrastructure,* eds Brian Kahin and Charles Nesson, MIT Press, Cambridge, Mass., 1997, pp. 205-234.

[68] World Intellectual Property Organization, *WIPO Copyright Treaty,* adopted by the Diplomatic Conference on December 20, 1996, WIPO 1996.

[69] An example of the implementation of the World Intellectual Property Organization (WIPO) treaties is the Australian *Copyright Amendment (Digital Agenda) Act* 2000 which together with the *Copyright Amendment (Moral Rights) Act* 2000 amended the Commonwealth *Copyright Act* 1968. These amendments include statutory moral rights, amendments to the fair dealing provisions, and the introduction of a new transmission right.

[70] World Intellectual Property Organization, *Basic Proposal for the Substantive Provisions of the Treaty on Intellectual Property in Respect of Databases to be Considered by the Diplomatic Conference Geneva, December 2 to 20 1996,* 30 August, 1996. WIPO proposed that facts or data in a database could be copyrighted. The extension of ownership over facts, with strict liability for infringement placed onto Internet Service Providers, would override fair use and free competition. It would increase monitoring and privacy interference, and protect large database operators.

been given copyright protection but case law has varied significantly on the matter.[71] The 1992 European Commission Directive on Database Protection has gradually been adopted in European Union member countries. The protection of data itself as a form of intellectual property is a major change to copyright law. The extension of copyright to cover data would have some effect on ownership of the content in records if they are classed as a database for the purposes of copyright law.

International copyright reforms indicate a continuing protection of material in non-interactive form, with new rights to cover transmission of material over the Internet. Increased protection has continued to favour copyright owners at the expense of users, compounded by licensing agreements and other forms of contract that modify exceptions granted under copyright law.[72]

Infringement and enforcement of copyright

The new right of communication makes works that are digitally transmitted without the owners' authorisation an infringement of the communication right (Article 8 of WIPO). Generally copyright infringements are due to unauthorised transmission or downloading of protected data or programs.

---

[71] The concept of copyright arising from 'added value' to facts through creative effort, has not been interpreted consistently by the courts. In the United States, names, addresses and phone numbers have not been given copyright protection. If copyright in facts is accepted in the United States, it would overturn the 1991 US Supreme Court decision in *Feist Publications Inc. v Rural Telephone Service* 499 US 340 (1990), as discussed in Chapter 5, footnote 53. In an Australian case regarding originality of facts, English rather than American precedents were used. In *Desktop Marketing Systems Pty Ltd v Telstra Corporation Limited* (2002) FCAFC 112, Telstra argued that compiling a telephone directory database required intelligence and effort while DTMS argued that it was only a collection of data. The judge used English precedents that have interpreted timetables as original works, and made it clear that database rights subsisted in the telephone directory. In the Netherlands in *KPN v Denda* a telephone directory was given copyright protection on the basis of the substantial investment in its production. See Dirk Visser, 'The Database Right and the Spin-off Theory', in *E-commerce Law: National and Transnational Topics and Perspectives*, eds Henk Snijders and Stephen Weatherill, Kluwer Law International, The Hague, London, New York, 2003, pp. 105-110.

[72] For a comment on the US situation, see US-InterPARES Project, *Findings on the Preservation of Authentic Electronic Records,* p. 86.

One must first establish that there is a copyright 'work' involved, and that it has been infringed.[73]

The notion of copying from the 'original' is nonsensical, as the copy is identical to the 'original', in terms of its content. However, original in its recordkeeping definition means the one that has all its meaningful elements, including its recordkeeping metadata. In the amended Australian Copyright Act to copy or to reproduce are used synonymously. The copyright concern is that an exact copy of something belongs to someone else; the issue of being a corrupted copy is relevant to an authentic record and contravenes the creator's moral rights of integrity.

The exclusive right of authorising any communication to the public, 'making available' provides the proprietor with a potential remedy, that is, the person making it available is the infringer. Reed claims that many of the lacunae in law relating to commercial Internet activities can only be filled by laws such as unfair competition and trade reputation, based on concepts of wrongful behaviour rather than property concepts. One can also use contract law, and identify the user or the rightful owner of an electronic publication via electronic signatures. Technological approaches to copyright protection are also relevant to enforcement (see below).

Technological protection of copyright

Technological means of protecting intellectual property have evolved from an early focus on encrypted content to the use of intellectual objects with controls over use. Locking out users include the use of password protection and hardware devices. Legal liability for circumvention of these devices is considered critical to copyright on the Internet.[74] There are concerns on how fair dealing can apply if all copyrighted material is protected by technical means.[75] The WIPO Articles 11 and 12 introduce a requirement for effective legal remedies for the removal of any technological means of circumventing copyright. However, the WIPO articles on technological circumvention of copyright may also affect 'the ability to make copies when migrating from one storage technology to another, and to reformat,

---

[73] Gordon Hughes and David Cosgrove, 'The Internet - Legal Questions', *Law Institute Journal*, vol. 69, no. 4, April 1995, pp. 326-327.

[74] In Australia, the *Copyright Amendment (Digital Agenda) Act* 2000 s 16B prohibits the removal or alteration of electronic rights management information. Copyright management information is also agent and use metadata.

[75] 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. 106.

thereby creating derivative works when moving from one software technology to the next.'[76] From a recordkeeping perspective technological circumvention provisions may present an obstacle to long term digital preservation which can only be a reproduction of an original work and may include migration of proprietary software and record metadata. Where copyright legislative exemptions for archival preservation exist they are frequently based on a custodial model that requires the archives instituition to have physical custody of the copyrighted work for the exemptions to apply.[77] The preservation of an electronic record must be considered at the time of a record's creation when it is unlikely to be in the physical custody of an archival organisation rather than after the expiration of copyright, for example, seventy years after the author's death.[78]

The prohibition on circumventing the technological devices in the United States is found in the *Digital Millennium Copyright Act* 1998 (US) s 1201(a)(1)(A) which provides that 'no person shall circumvent a technological measure that effectively controls access to a work protected under this 'title'. Excluded are works that the Librarian of Congress determines.'[79] The purpose of the exemption by the Library of Congress is to ensure that particular classes of works to which users are, or are likely to be, adversely affected in their ability to make noninfringing uses due to the prohibition on circumvention of access controls are allowable.[80] The Act

---

[76] US-InterPARES Project, *Findings on the Preservation of Authentic Electronic Records,* p. 84, (quoting from Committee on Intellectual Property Rights and the Emerging Information Infrastructure, *The Digital Dilemma: Intellectual Property in the Information Age*, National Academy Press, Washington DC, 2000, p. 119.)

[77] Ibid., p. 85; Filip Boudrez and Sofie Van den Eynde*, Archiving Websites,* State Archives of Antwerp, Antwerp-Leuven, 2002, p. 91.

[78] An exception for libraries and archives in the US in the last twenty years of copyright protection would be of little use for preservation. US-InterPARES Project, *Findings on the Preservation of Authentic Electronic Records,* p. 86.

[79] Brennan, 'Simplification, Circumvention, Fair Dealing and Australian Copyright Law', p. 116.

[80] For example, October 28, 2003, the Librarian of Congress, on the recommendation of the Register of Copyrights, announced the classes of works subject to the exemption from the prohibition against circumvention of technological measures that control access to copyrighted works. These included: '(3) Computer programs and video games distributed in formats that have become obsolete and which require the original media or hardware as a condition of access. A format shall be considered obsolete if the machine or system necessary to render perceptible a work stored in that format is no longer manufactured or is no longer reasonably available in the commercial marketplace.' United States Copyright Office, *Rulemaking on Exemptions from*

targets circumventing an access control mechanism to a work rather than the unauthorised use. However, in many cases access and security measures may be inseparable.[81] In Australia only the manufacture and supply, but not the use, of a circumvention device or service are proscribed by the *Copyright Act* 1968 (Cth). A circumvention device or service may be supplied for certain 'permitted purposes' which include copying by libraries and archives. The Australia/US Free Trade Agreement (AUSFTA) requires Australia to amend its provisions to operate as in the US, in particular the introduction of sanctions against circumventing a technological protection measure, and limitations on exceptions for circumvention.[82] While legal conformity provides for greater consistency between countries that are parties to a trade treaty such as AUSFTA it may also remove Australian provisions that are more advantageous to the preservation of records.

'Rights management information' (RMI) in the WIPO treaties provide sanctions for deliberate removal or tampering with copyright identification information electronically attached. The use of technology to protect copyright by fencing out unauthorised users has involved rights management software of two kinds. One that manages the rights, that is, the transactions dealing with the use of a digital object some of which need full identity disclosure, and the other that reduces 'usage' uncertainty.[83] Rights systems maintain data on the identity of the record creators. These systems duplicate recordkeeping metadata. The 'rights community' could also be analysed in the relationship model in terms of the copyright owner and the user, and other rights such as privacy.

Prohibition on Circumvention of Technological Measures that Control Access to Copyrighted Works, The Recommendation of the Register of Copyrights.

[81] Liong Lim, 'US Digital Millennium Copyright Act', *Internet Law Bulletin*, vol. 2, no. 1, Feb. 1999, pp. 11-14.

[82] Australian Copyright Council, *Access to Copyright Material in Australia and the US.* US court decisions on copyright have been in many instances quite different to Australia.

[83] Peter Higgs, 'Privacy Implications of On-line Intellectual Property Protection', in Papers from *The New Australian Privacy Landscape*, Faculty of Law, Continuing Legal Education, The University of New South Wales, 14 March 2001. Here the term 'rights' is used in relation to the rights of owners of copyright (rather than rights of users), who want their work protected which may lead to privacy infringement of users.

7.2.3 Web access to public records

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

David Roberts, in 1995 in *Documenting the Future*, described future networked access to documents themselves: users login as 'guest users' with access rights and restrictions, data will be secured with 'firewalls' to separate them from publicly accessible parts, and applicants use the retrieval tools of the agency's recordkeeping system with necessary security safeguards, therefore reducing time and cost for the agency.[84] This scenario assumed that governments would release the records, provide safeguards, and secure the records as time bound into the future and make decisions on archival requirements. Networked access to an agency's records for the public user has not been implemented, and archival authorities are beginning to take custody of electronic records. Electronic access to government data, will involve some continuum in access, and consideration of bringing the access provisions of all legislation dealing with it together, that is, the public right to know as expressed in FOI and the right to privacy in privacy legislation. However, at present access in FOI, archival, and privacy legislation in many jurisdictions is often fragmented, and at times conflicting.

Which government records are made available will depend more on political will rather than the technology of the Internet. This is clearly visible in the watering down of FOI legislation in many countries due to security fears,[85] and the privatisation of government activities which have led to the reduction of the ambit of FOI.

7.2.4 Privacy and web 'business' transactions

There are good arguments for stronger privacy legislation for Internet electronic transactions. These include:

---

[84] David Roberts, *Documenting the Future, Policies and Strategies for Electronic Recordkeeping in the New South Wales Public Sector,* The Archives Authority of New South Wales, Sydney, 1995.

[85] Moira Paterson, *Freedom of Information and Privacy in Australia: Government and Information Access in the Modern State,* LexisNexis Butterworths, Chatswood, NSW, 2005, p. 8.

- the compilation of customer profiles derived from online contracts;
- unauthorised access to, distribution of and tampering with personal data in electronic networks with the possibility of destroying or interfering with the data (which means the record's integrity is threatened); and
- global data matching and surveillance of users of networks by government and between governments, law enforcement agencies and commercially-interested parties using private data dispersed amongst providers.

The relationships between the traditional players, and their respective rights and duties, may not translate into the online world. Contract and licensing have been used to bypass privacy, as well as copyright, defamation and censorship laws, but government contractors should be required to abide by privacy legislation.[86] There are often limitations in the privacy legislation in its application to the Internet, for example in Australia personal information is defined as '... an individual whose identity is apparent' (*Privacy Act* 1988 s 6) when identity is not apparent but may reside in the log of web access held on a server.[87]

In the European Union the scope of the definition of personal data is extremely wide, but the interpretation in relation to individual member states varies. For example, under Belgian data protection law 'personal data' is every piece of information regarding an identified or identifiable natural person. Data is identifiable if someone, the data controller or a third party, is able to link the data to a natural person using any reasonable means. An IP address is personal data as it is reasonably possible for an ISP to determine an 'identifiable' person to whom it belongs, even though the archivist may not be able to achieve this. The Netherlands has not taken the strict Belgian interpretation of identifiable personal data; it does not consider that in all cases IP addresses are personal data. The Dutch view is that the body processing the personal data has to have the ability to identify an individual via his/her IP address. An archivist could argue that, unlike the ISP, he/she does not have additional information to identify a person.[88]

---

[86] Gordon Hughes, 'Our Rapidly Expanding Privacy Obligations', *Law Institute Journal*, vol. 75, no. 6, July 2001, p. 58. Government contracts in Australia have to be consistent with the privacy regulations of Commonwealth agencies.

[87] Graham Greenleaf, 'Privacy Principles - Irrelevant to Cyberspace?', in *Internet Law Anthology*, ed. Peter Leonard, Prospect Intelligence Report, Prospect Publishing, Sydney, 1997, pp. 129-138.

[88] Boudrez and Van den Eynde, *Archiving Websites*, pp. 78-79.

Privacy: international context

The 1980 OECD *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, the 1985 *Declaration on Transborder Data Flows* and the 1998 *Ministerial Declaration on the Protection of Privacy on Global Networks* represent international instruments on the collection and management of personal information.[89] Ensuring privacy in Internet transactions is a key consideration internationally. For mechanisms to be effective international regulations and agreements, not domestic, are an imperative. Without international consensus privacy in networks will not work.

> With increasing globalisation of e-commerce, privacy protection is rapidly becoming a transnational issue. As we do more and more transactions on-line, and as organizations contract out more and more functions - often offshore - we can no longer protect our privacy with purely domestic laws. Also, even where privacy regulations address wholly domestic activities, the standards expected are drawn from comparative international experience.[90]

The OECD in 1998 highlighted privacy as a fundamental requirement to give people confidence in the digital marketplace. It concluded that governments have fundamental responsibilities in this area, and that much is expected from, and dependent on, private sector initiatives.[91] Privacy is an area where international convergence is the model. However, there is considerable variation in how privacy is interpreted in online contexts. With the notable exception of the United States, privacy legislation has expanded in the last two decades. The United States 'Safe Harbor' arrangement with the European Union is a self-regulatory scheme which provides certain privacy safeguards and requires US companies that intend to receive personal data from EU countries to be registered within the scheme.[92] However it is not considered a suitable model by privacy advocates.

---

[89] OECD, Information Security and Privacy documents, 2005.

[90] Nigel Waters, 'A Comparative Analysis of Australian Privacy Laws with Special Reference to the Concept of "Adequacy" for the Purposes of the European Union Data Protection Directive', in Papers presented to *The New Australian Privacy Landscape*, Faculty of Law, Continuing Legal Education, The University of New South Wales, 14 March 2001 (no pagination).

[91] OECD, Ministerial Declaration on the Protection of Privacy on Global Networks, OECD Conference*, A Borderless World: Realising the Potential of Global Electronic Commerce,* Ottawa, 7-9 October 1998.

[92] The operation of Article 25 of the Data Protection Directive (95/46/EC) requires that member states take measures to prevent any transfer of personal data to a country that the European Commission finds provides inadequate privacy

Australian privacy law has drawn from external jurisdictions and international agreements and is a good example of international legal models that operate across borders.[93] The *Privacy Act* 1988 (Cth) is based on the OECD principles, and like intellectual property has an international context that is important in terms of Internet developments. The extension of Australian privacy law to the private sector brought Australia in line with international approaches. In relation to its international obligations, the *Privacy Amendment (Private Sector) Act* 2000 (Cth) has within its main objects focused on Australia's international obligations.[94] The national principles of particular relevance to the Internet are the option to remain anonymous when entering transactions (NPP8) and controls on transfers of personal information out of Australia (NPP9).[95] The extra-territorial operation of the Act covers personal information overseas if there is an organisational link with Australia, but it only covers Australians.

---

protection. An alternative transfer method from EU countries to other countries is under EU model clauses. Sparrow, *The Law of Internet and Mobile Communications: The EU and US Contrasted*, pp. 12-38.

[93] Hughes, 'Our Rapidly Expanding Privacy Obligations', p. 60. In fact the European Commission undertakes adequacy assessments of national privacy laws, and did not consider the amendments to the *Privacy Act* 1988 (Cth) as adequate for data transfers to Australia from Europe.

[94] *Privacy Amendment (Private Sector) Act* 2000 (Cth) s 3.

[95] Graham Greenleaf, 'Privacy Principles: Problems in Cyberspace - Likely Areas of Controversy and Interpretation', in Papers from *The New Australian Privacy Landscape*, Faculty of Law, Continuing Legal Education, The University of New South Wales, 14 March 2001, p. 7. There are some transactions where anonymity may be desirable. Pseudonyms have been suggested as a preferable principle to anonymous transactions as certification authorities could hold the real names separately to prevent their disclosure. Transfers of personal information out of Australia are exempted from obtaining consent in s 9(e)(ii) of the *Privacy Act* 1988 (Cth). The EU position is found in *2002/58/EC on Privacy and Electronic Communications,* '(9) The Member States, providers and users concerned, together with the competent Community bodies, should cooperate in introducing and developing the relevant technologies where this is necessary to apply the guarantees provided for by this Directive and taking particular account of the objectives of minimising the processing of personal data and of using anonymous or pseudonymous data where possible. (33) Member States should encourage the development of electronic communication service options such as alternative payment facilities which allow anonymous or strictly private access to publicly available electronic communications services, for example calling cards and facilities for payment by credit card.' *Official Journal of the European Communities*, L 201/37, 31.7.2002. See also Michael Kirby, 'Privacy in Cyberspace', *University of NSW Law Journal*, vol. 21, no. 2, 1998, pp. 323-33.

As with other Internet legal issues if one country does not protect privacy, it becomes unenforceable across borders. Even if principles are the same, substantive differences may apply to different categories, for example a consumer may have to consent or follow opt-in or opt-out provisions. Standards may be insufficient, for example many American companies agreed to adhere to the OECD standards but few changed their practices. A detailed voluntary international privacy code adopted by merchants and consumers with specific responsibilities, along with rights of consumers, some oversight of the activities, as well as practical remedies such as auditing and electronic dispute resolution mechanisms, are required. Adjudication can be implemented through private sector arbitration, but may still not meet the adequacy test of the European Union.[96]

Privacy and access policy for Internet transactions

The management of access on the Internet, and privacy in particular, involves control over to whom information is released, and how it is construed or to what use it is put, and how long it is retained. Policy decisions should precede technological solutions. Examples of Internet privacy policies include private arrangements. In the United States negotiated privacy between user and provider is available by paying a higher price for greater privacy. User privacy in user-provider agreements arrange that the provider will only review messages if there is some suspicion of illegality.[97]

The World Wide Web Consortium has developed a standard that compares a user's privacy preference with that of a website enabled with the standardised privacy policy. This approach relies on the truthfulness of the policy, and for organisations to 'opt in'.[98]

---

[96] Robert Gellman, 'Conflict and Overlap in Privacy Regulation: National, International, and Private', in *Borders in Cyberspace: Information Policy and the Global Information Infrastructure,* eds Brian Kahin and Charles Nesson, MIT Press, Cambridge, Mass., 1997, pp. 255-282.

[97] Lance Rose, *Netlaw: Your Rights in the Online World,* Osborne McGraw-Hill, Berkeley, 1995, pp. 171-185.

[98] W3C, 'The Platform for Privacy Preferences Project (P3P)', 2000, revised 2005, W3C.

Technological and recordkeeping solutions to Internet privacy

Legislation is only one element of privacy protection.[99] A recordkeeping technique to provide evidence of privacy infringements is the use of audit trails or event histories that log or trace who has had access or made any amendments and when to a record.[100] Security controls or 'privacy enhancing technologies' may enhance privacy protection but they cannot guarantee it.[101] For example public key cryptography is designed to ensure security from unauthorised access to personal data on the basis of requiring a third party to control identity certification, but relies on an organisation or person who can be trusted with the keys to the encryption regime. Public key management systems act as trusted mediators between senders and recipients to certify a link between individuals and their public keys. Both the trusted mediators and the keys must themselves be controlled, thus requiring a hierarchical chain of trust. The danger is that if the trusted authority's owner (eg the government or a private organisation) has control over the decryption keys, it can build an extensive identification system and authorise its use. The cryptographic key can also be opened by a court order revealing unnecessary personal information linked to an individual's key. Even with secure key management, a legal warrant may allow law-enforcement agents, employers, or a system owner to have access to keys, thus severely compromising individual privacy.[102] Anonymous remailers

---

[99] See also Livia Iacovino, 'Regulating Net Transactions: the Legal Implications for Recordkeeping in Australia', in *Place, Interface, and Cyberspace: Archives at the Edge,* Proceedings of the Australian Society of Archivists Conference, Freemantle, 6-8 August, 1998, Australian Society of Archivists Incorporated, Canberra, 1999, pp. 103-123.

[100] Tracking provides an auditable trail of record transactions, ensuring that event histories are part of the record. 'Tracking' is defined in the ISO records management standard as 'creating, capturing and maintaining information about the movement and use of records'. ISO, International Standard ISO 15489-1, *Information and Documentation, Records Management*, Part 1, p 3.

[101] 'Privacy-enhancing products are those that have been designed in a way that aims at accomplishing the largest possible use of truly anonymous data.' European Commission, Data Protection Working Group, WP37, *Working Document: Privacy on the Internet - An integrated EU Approach to On-line Data Protection,* November 2000, Article 29. See also Philip Agre, 'Beyond the Mirror World: Privacy and the Representational Practices of Computing', in *Technology and Privacy: the New Landscape,* eds Philip Agre and Marc Rotenberg, MIT Press, Massachusetts, 1998, pp. 29-62.

[102] See for example, the *Telecommunications (Interception Act)* (Cth) 1901 which, pursuant to a warrant allows access to the encryption key. Natalia Yastreboff, 'Encryption and Australian Government Policy', in *Internet Law Anthology*, ed.

allow identifying elements of communications to be omitted without attribution to any recipient, and together with encryption, one can be totally anonymous. However, a blanket approach of this kind ignores the necessity of identification for record reliability and authenticity purposes.

7.2.5 Evidence in web 'business' transactions

If laws of evidence are particularly prone to their cultural origins, in the global context there is an opportunity for securing universal approaches across legal systems. The Internet raises questions about the legal status of documents as evidence outside national boundaries. The contractual nature of many business transactions necessitates that their evidential qualities be present. At this stage, there is insufficient case law to know how the courts will deal with records as evidence from the Internet.

The Internet is a packet switching network; data can be broken up and routed to their destination along the most suitable path. As the message is reconstructed at its point of destination, interception and alteration may occur during its transmission, endangering the integrity of the communication. In addition, security in a recordkeeping context means ensuring that records retain their integrity over time. For these reasons, the evidential issues relevant to electronic transactions on the Internet are often submerged under discussions on security, encryption and electronic signatures. Secure systems adopting encryption technologies are central to the success of the Internet for recordkeeping. National governments have all developed technologies for this purpose, not often without controversy.[103] The most important issue is the need for businesses and archival authorities to be able to decrypt data, an essential issue for records to be accessible over time.[104]

Peter Leonard, Prospect Intelligence Report, Sydney, Prospect Publishing, 1997, pp. 108-115; David J. Phillips, 'Cryptography, Secrets, and the Structuring of Trust', in *Technology and Privacy: the New Landscape*, pp. 243-276.

[103] The Australian Taxation Office, *Tax and the Internet,* in August 1997 raised a number of recordkeeping issues, including the acceptance of encryption of the data content. Australian Taxation Office, *Tax and the Internet,* Discussion Report of the ATO Electronic Commerce Project, AGPS, Canberra, August 1997.

[104] National Archives of Australia, *Recordkeeping and Online Authentication and Encryption,* Archives Advice 64, September 2003/Revised May 2004; National Archives of Australia, *Recordkeeping and Online Security Processes:*

Laws of evidence: International context

The ability of systems linked to the Internet to retrieve transactions with all their contextual attributes is uncertain, but is being addressed by new technologies. Recognition of the need to maintain evidence, including the completeness of data that forms part of an Internet transaction for potential legal proceedings, has been recognised internationally by the OECD, and is provided for in their *Guidelines for the Security of Information Systems*, including provision for the diverse rules of admissibility in legal systems of different countries.[105] In addition, the Electronic Transactions and Signature Acts in many countries are modelled on the international UNCITRAL model.

The laws of evidence are relevant to the admissibility of documents and records as evidence by the courts, that is, they are the rules which determine what and how records may be introduced into legal proceedings. Electronic information, used in the course of a business or social activity, functions as a record, and may be admissible as evidence.[106] Therefore the admissibility of Internet transactions would appear to be covered in jurisdictions which include rules of evidence that include business and computer records provisions.[107]

Not withstanding the probability that Internet transactions would be legally admissible, the view expressed by a Canadian expert group on law, audit and archives is that electronic transactions need legislative certainty

---

Guidelines for Managing Commonwealth Records Created or Received Using Authentication and Encryption, May 2004.

[105] OECD, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, May 2004.

[106] Conni Christenssen, 'The Intranet/Recordkeeping Technical Interface', 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. 19.

[107] Two features of Australian federal evidence legislation which are particularly relevant to transactions on the Internet are the abolition of the original document rule, and provisions for easier proof of, and presumptions about, business and official records, and the use of email, fax and other means of communication. The presumptions opened the way for the admissibility of Internet transactions endorsed in the Attorney-General's Electronic Commerce Expert Group report. Electronic Commerce Expert Group, *Electronic Commerce: Building the Legal Framework, Report of the Electronic Commerce Expert Group to the Attorney General,* 31 March 1998, Recommendation 9, p. 112.

in the normal course of business. This view has in fact been endorsed in most countries.[108] For example the United States, Canada and the European Union member countries have opted to enact specific legislation for electronic communications and contract via electronic signature and electronic commerce legislation.[109] In Australia the technology-neutral *Electronic Transactions Act* 1999 (Cth) is centred on ensuring that electronic communications have legal validity, in particular, but not exclusively, in contractual circumstances.[110] It establishes the basic rule that a transaction is not invalid because it took place by means of an electronic communication and is based on two principles: functional equivalence (also known as media neutrality) 'that transactions conducted using paper documents and transactions conducted using electronic communications should be treated equally by the law and not given an advantage or disadvantage against each other', and technology neutrality that ensures 'the law should not discriminate between different forms of technology for example, by specifying technical requirements for the use of electronic communications that are based upon an understanding of the operation of a particular form of electronic communication technology'.[111]

---

[108] National Archives of Canada, *The Keeping of Business Records for Law, Audit and Archives: A Report on the Experts' Meeting*, June 10-11, 1999, Ottawa, Ontario, NAC, Canada, June 1999, p. 3.

[109] See Jos Dumortier, 'Directive 1999/93/EC on a Community Framework for Electronic Signatures', pp. 33-65 and Arno R. Lodder, 'Directive 2000/31/EC on Certain Legal Aspects of Information Society Services, in particular Electronic Commerce, in the Internal Market', pp. 67-93, 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. For a discussion of the Italian digital signature legislation, see 'La Gestione Informatica nell'ordinamento Giuridico Italiano' in Maria Guercio, *Archivistica Informatica*, *I Documenti in Ambiente Digitale,* Carocci, Rome 2002, pp. 155-221. On Canadian and US electronic signature and online contract laws, see *E-Commerce in the World: Aspects of Comparative Law*, coordinated by Jean-Pierre van Cutsem, Arnaud Viggria, Oliver Güth, Bruylant, Brussels, 2003, pp. 156-168 and pp. 320-325, respectively.

[110] The *Electronic Transactions Act* 1999 (Cth) is based on the recommendations of the Electronic Commerce Expert Group, which reported to the Attorney-General in March 1998. See also *Electronic Transactions Act* 1999 (NSW) and *Electronic Transactions Act* 1999 (Vic) which are modelled on the Commonwealth Act.

[111] *Revised Explanatory Memorandum, Electronic Transactions Bill 1999,* 'General Outline', p. 1.

Legislation supports the need to be able to recreate records, not just data.[112] The *Electronic Transactions Act* 1999 also requires that records be accessible for as long as the record needs to be in existence (see ss 9, 11 and 12) 'at the time the information is given, it must be reasonable to expect that the information would be *readily accessible so as to be useable for subsequent reference*'.

> ... The readily accessible requirement ensures that others will be able to access the information contained in the electronic communication and that transactions are not subsequently vitiated by a lack of access to the information … The notion of readily accessible is intended to mean that information contained in the electronic communication should be readable and capable of being interpreted. Similarly, it is intended that software necessary to allow the information to be read should be retained. This may be the version of the software used to create the message or subsequent versions of the same or different software that is capable of rendering the information readable. The concept of useable is intended to cover use by both humans and machines. It is intended to deal with the useability of information, which is more than just the receipt of the electronic communication.'[113]

Thus the *Electronic Transactions Act* 1999 (Cth) supports authentic Internet records. Other legal, business and societal requirements continue to operate for ascertaining how long to keep the communication. However the Act does at least provide a minimum record retention requirement in electronic form. European electronic and digital signature legislation does not address record authenticity; rather it emphasises detailed rules for transmission in time but not over time.[114]

In terms of legal enforcement in the Internet context, current approaches as outlined in this chapter include the further development of international law both public and private, the application of international model laws and treaties which have been adapted to local conditions by their adoption into domestic legislation (for example, the UNCITRAL model used for the national Electronic Transactions Acts, and the OECD and European Union directives on privacy and national privacy legislation), or simply enforcing domestic laws by claiming breaches occurred within one's jurisdiction. Self-regulation models have also provided an alternative to increased

---

[112] For example in Australia, in relation to s 262A of the *Taxation Act* 1936 (Cth), Draft Taxation Ruling 97/D4 covers computerised recordkeeping system controls and specifies that data collected and how it has been used must be able to be recreated.

[113] *Revised Explanatory Memorandum, Electronic Transactions Bill 1999,* p. 26.

[114] InterPARES 1 Project, *Italian Research Team Report*, 2001, prepared by Maria Guercio, p. 1.

legislative regulation. Thus the combination of self-regulation and traditional legal sanctions are likely to work best with electronic information which is no longer confined to one jurisdiction.

Ownership, access, privacy and evidence have also needed adjustment to the Internet. There are international frameworks now established for intellectual property, electronic commerce and privacy, and national changes are slowly moving to accommodate these international trends. The risks of not creating reliable and authentic records that may need to be retrievable with all their recordkeeping features over time will continue to be the central issue for recordkeeping regulation.

Electronic transactions legislation can be applied to recordkeeping at the micro-level of business transactions, but not as evidence of legal and social obligations within a community of common interest. Thus the model advocated for identifying the legal obligations of recordkeeping participants online follows the school of legal thinking that in recent years has turned to the law of obligations for legal analysis, but has not itself extended this approach to the Internet.