THE ROLE OF INFORMATION TECHNOLOGY LAW IN AUSTRALIAN INTERNET REGULATION

Olujokè E Akindemowo*

THE EVOLUTION OF INFORMATION TECHNOLOGY LAW

The Role of Categorisation

The urge to organise is an instinct particularly developed in the human psyche. As the rules regulating human existence proliferated, the categorisation of these rules into distinct groupings became commonplace among those concerned with the study of law. The discipline[1] of law is thus divided into fields that are in turn sub-divided into subjects which may be further sub-divided into topics.

The discipline of law is comprised of a complex array of constantly evolving norms grouped into different fields, ranging from the established - some of which have distinguished pedigrees measured in centuries - to the progeny of technological development so recently evolved as to be barely recognised as a field in their own right.

Historical Controversies

Information Technology Law, one such of such progeny, is a field whose evolution has been so controversial that its existence has been denied by some.

Some commentators take the view that issues raised by the use of computer technology are neither novel nor significant, asserting that existing laws are sufficient to meet whatever contingencies that may arise. Others seem at first to similarly deny the existence of a field, but

* LL.B (Ife), B.L (Nig), LL.M, Ph.D (Lond), Lecturer in Law, University of Western Sydney, Nepean.

[1] For the sake of clarity, it is noted that the term discipline is used here to refer to a branch of instruction or learning, and a field to a range or area of study or operation.

on closer examination describe in fact the existence of phenomena that go at least some way towards justifying the existence of such a field[2].

The argument has also been made that there is no need for such a field of law because the issues raised are few in number, unlikely to endure what is sometimes referred to as its "evolutionary period", and may be satisfactorily disposed of on an ad hoc basis. The undesirability of resorting to the enactment of legislation except in the most serious situations is often mentioned as a bolstering point in this regard.

On closer examination however, it becomes evident that these arguments are based on the following inaccurate or confused premises:

(i) that to recognise the existence of such a field is to claim that a non-intersecting category, distinct in every way, exists;

(ii) that recognising the field as such will concede that it is no longer evolving and that its boundaries are immutable;

(iii) that arguments for the existence of the field depend on the identification of issues that are overwhelmingly novel and unprecedented in every respect;

(iv) that arguments for the recognition of the field in effect call for the passing of sui generis legislation.

Arguments about whether issues raised are overwhelmingly novel, or require the wholesale amplification of statutory law[3], are beside the point. The crux of the argument is that the recognition of such a field requires the creation of a new sub-category of the

2 The fact that novel issues arise in the context of certain fields is conceded, but they are discounted as being more properly considered in the context of whatever (more) established field they appear at first sight to arise from. In relation to this, see the functions of categorisation in law detailed below.

3 It is a fallacy to assume that the only means of correcting lacunae in the law are statutory amendments - the common law may be flexible enough to cover the situation albeit in an unprecedented manner. The difficulty with unprecedented applications is that they may be overruled where they are deemed an usurpation of the legislative function. Thus in the absence of a court decision, or statutory amendment legal advice on the matter may be tentative at best.

discipline of law. The real question is whether such categorisation can be justified.

Categorisation is employed within the discipline of law:

(i) to provide a pragmatic reflection of the common features, policy considerations or historical connections of a group of matters; and

(ii) as a convenience measure to:

(a) facilitate the identification of common features, trends and relationship links;

(b) simplify the process of locating or applying relevant principles within the discipline;

(c) define the minimal scope of inquiry of investigations and provide a choice of strategies;

(d) provide a rallying point for investigators and indicates the background knowledge or skills that may be required for a thorough comprehension of matters raised; and

(e) provide a context from which matters may be evaluated from a relative and more accurate perspective.

It is relevant to note here that none of the categories or sub-categories of the discipline of law are static because all are subject to constant, if incremental, development. Those directly related to technological change, however, evolve at a much faster rate - their indicated scope must be regarded as flexible indicators on a continuum rather than fixed exclusive boundaries. It is also important to remember that these categories are not arranged in a linear or hierarchical fashion - they intersect in various ways and may be arranged in sub-groups in different combinations. Sociological scholarship provides some support for the contention that fields of study are evolutionary and often accidents of history, rather than static or inflexible categories[4].

[4] See for example A King, "The Future as a Discipline and the Future of the Disciplines", JN Black, "Sclerotic Structures and the Future of Academic Organisation"; and K

A Vitally Relevant Field

From its origins as a high maintenance, computational tool used for specialised scientific purposes, the computer developed into a general-purpose tool of extraordinary versatility and wide application. Its influence has become so pervasive that it is, in the more developed Western societies, an inextricable part of ordinary life. This has meant that issues arising from the use of computers or the Internet have tended to be socially and/or politically significant, and it is such issues that are the invariable subject of field categorisation.

In any case, the existence of information technology law as a field in the discipline of law can no longer be denied because it raises issues which:

(i) have a significant common denominator - legal issues raised by the use of computers;

(ii) are significant because they are novel in themselves, or require novel applications of existing concepts[5];

(iii) if systematically arranged in this context, would make ill-informed legal analyses less likely, and facilitate the identification of potential legal risks; and

(iv) if thus categorised, would reflect realities encountered in practice[6].

Valaskakis, "Eclectics: Elements of a Trasndisciplinary Methodology for Future Studies", in GEW Wolstenholme and M O'Connor (ed) *The Future as an Academic Discipline held at the Ciba Foundation: Symposium No. 36*, Amsterdam, Elsevier, 1975 at 45-47, 107-114 and 122-124 respectively; also R Dore, "Why Visiting Sociologist Fail" (1994) 22 *World Development* 1425-1436.

5 Which in turn have created legal uncertainties and made the re-evaluation or refinement of specific concepts necessary. It is relevant to note in this regard that the refinement of legal concepts is limited in practice by type or level of degree of judicial activism that is deemed permissible in the jurisdiction concerned. The point at which "refinements" of concept become "substantial changes in principle" and hence the usurpation of the legislative function will vary according to the circumstances.

6 Such as (a) the specialist information technology law/computer law divisions in law firms; (b) the existence of university information technology law/computer law courses taught at undergraduate and postgraduate level; (c) the circulation of information technology law/computer law journals such as the *Computer Law and Security Report* (CLSR), the *Computer and Telecommunications Law Review* (CTLR), the *Journal of Law and Information Science* (JLIS); (d) the existence of national and international information

The field thus includes subjects such as computer-related commercial obligations and liabilities, privacy and data protection, the legal nature and admissibility of computer-generated evidence, jurisdictional issues, computer crime, and of course, the regulation of Internet abuses. The subjects cover a wide range of topics, many of which are directly relevant to the Internet. Following therefore, is a sampler of such topics, in further illustration of the role and pertinence of the field to contemporary Internet-related legal concerns.

A SAMPLER OF INTERNET-RELATED RISKS

Electronic Commerce

Electronic commerce in general raises issues that have roused concerns in many quarters[7]. One topic of especial interest relates to the legal risks of electronic contracting.

Contracting Risks:

Electronic Documents

The data processing and storage capacities made commonplace by today's computers have introduced a forum which is neither tangible nor a form of verbal expression: electronic messages - which raise the question of whether there can be such a thing as "electronic writing" or an "electronic document" for legal purposes.

---

technology law/computer law associations e.g. the NSW Society for Computers and Law, and (e) regular occurrence of national and international information technology law/computer law conferences an example of which is the IASTED International Conference on Law & Technology held in Hawaii in 1999.

[7] The Attorney General's Department and the National Office of the Information Economy (NOIE) are two federal level entities vitally involved in the monitoring and investigation of such matters. Other bodies, such as consumer organisations are also monitoring developments - see for example the report published by the Federal Bureau of Consumer Affairs, *Untangling the Web: Electronic Commerce and the Consumer*, Canberra, AGPS, March 1997 and the report of the National Advisory Council on Consumer Affairs on *Consumer Protection in Electronic Commerce: Principles and Key Issues*, April 1998 (http://www.dist.gov.au/consumer/eleccomm/princip.html)

Some of these concepts have been re-defined for general legal use. The *Acts Interpretation Act* 1901 (Cth), for example, now provides that:

> "In any Act, unless the contrary intention appears:
>
> 'document' includes.... (c) any article or material from which sounds, images or writings are capable of being reproduced with or without the aid of any other article or device;
>
> 'record' includes information stored or recorded by means of a computer;
>
> 'writing' includes any mode of representing or reproducing words, figures, drawings or symbols in a visible form."[8]

The concept of the signature has also evolved in response to technological developments[9]. At a basic level, a signature identifies the signatory of a document and indicates the personal involvement of the signatory in the creation of the document. It also attests to the accuracy of the contents of the document and indicates the intention of the signatory to be associated with or bound by obligations in that document[10]. These identification and authentication functions, arguably the essence of a signature, may be performed by Personal Identification Numbers (PINs) and certain encryption functions[11] and biometric techniques, which are for this reason now commonly referred to as electronic signatures[12]. It is not however the case that

---

[8] See s25 *Acts Interpretation Act* 1901 (Cth). The *Evidence Act* 1995 (Cth) also provides that "document means any record of information, and includes.... (c) anything from which sounds, images or writings can be reproduced with or without the aid of anything else....".

[9] See for example *R v. Moore* (1884) 10 VLR 322, *Electronic Rentals Pty Ltd v. Andersoon* (1971) 124 CLR 27, and *Molodyski v. Vema Australia Pty Ltd* (1989) NSW Conveyancing Reports 55-446.

[10] On the legal effects of electronic signatures generally see A Mccullagh, P Little & W Caelli, "Electronic Signatures: Understand the Past to Develop the Future" (1998) 21(2) *UNSWLJ* 452-65, and M Sneddon, "Legislating to Facilitate Electronic Signatures and Records: Exceptions, Standards and the Impact on the Statute Book" (1998) 21(2) *UNSWLJ* 334-403.

[11] Used as digital signatures.

[12] For more on electronic signatures, and the developing Australian National Electronic Authentication Framework intended to facilitate the reliability, security and wider use of such signatures, see National Public Key Infrastructure Working Group, *Strategies for a Peak Body for and Australian National Electronic Authentication Framework: A Report Prepared for the National Office for the Information Economy*, April 1998(http://www.noie.gov.au/docs/npkiworkingpartyreport.html), also Standards Australia, *Strategies for the Implementation of a Public Key Authentication Framework (PKAF) in Australia*, 1996 (Report MP75, Sydney). See National Office for the Information Economy, *Establishment of a National Authentication Authority: A Discussion Paper* (Canberra, December 1998).

electronic signatures are equated with manual signatures in the general legal context. Although it is now no longer seriously doubted that the use of electronic methods in certain contexts is legally effective[13], it was recently suggested by the Attorney-General's Expert Group on Electronic Commerce (EGEC) that minimal legislation be enacted to remove lingering uncertainties about the legal efficacy of electronic signatures[14].

The UNCITRAL Model Law on Electronic Commerce, which was approved as an appropriate model for Australia by the EGEC, provides, for the avoidance of any doubt, that:

> "(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if
>
> (a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and
>
> (b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.
>
> (2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature."[15]

Provisions such as the above are playing a significant role in lessening the legal uncertainties affecting the efficacy of digital

---

[13] A binding contract, for example, may be formed through the exchange of a digitally written and signed offer and acceptance.

[14] Lest this operate as a hindrance to the development of electronic commerce - see the Final Report of the ECEG released 31 March 1998, especially the Executive Summary (Recommendations), recommendation one, and chapters two and three of the report in general (Attorney General's Department, Canberra, 1998, available at http://www.law.gov.au/aghome /advisory/eceg/ecegreport.html). See also the following publications of the Ministerial Council for the Information Economy, *A Strategic Framework for the Information Economy: Identifying Priorities for* Action (December 1998), *Towards An Australian Strategy For the Information Economy* (July 1998) which provide statements of the Australian Government's policy approach, and *Building the Information Economy: A Progress Report on the Enabling Legal and Regulatory Framework* (June 1998) which provides an up to date account of the legal and regulatory changes that have been targeted or implemented as a part of the Australian Government's strategy for the encouragement of the development of a vigorous information economy in Australia (all available at http://www.noie.gov.au/ecom/HOME/policy/policy.html).

[15] See Article 7 of the Model Law entitled "Signature".

documents because they ensure that legal requirements of form are satisfied. Recent amendments to statutory rules of evidence are also facilitating this objective by providing for the admissibility of such documents.

Concerning the question of whether the form of a formal document such as a deed can be similarly translated this will depend on the function and import attached to such form. The conventional form of a deed requires that it be signed, attested, sealed, and delivered. A signature and a seal both have the common function of authentication. The signature confirms that the signed document is the creation or expression of the will of the signatory, while the seal confirmed that the document was executed by will of such signatory. The authenticating functions which cryptography makes possible are today utilised in variety of ways that may be adapted to this context. The use of public and private encryption keys is one example - a specially selected string data, encrypted by means of the private key, embedded within the document could serve both purposes. Sealing at any rate is a strict requirement in few cases only. The traditionally vital role physical attestation played in centuries past has also been greatly lessened in recent times. The inconsistency between the tendency of computer and communications technology to promote remote (though on-line) transactions and the traditional nature of attestation which consists of the confirmation based on physical presence is therefore not particularly significant. Should the position have been otherwise, it would be arguable anyway that the visually assisted on-line simultaneous transactions made possible by video enhanced communications links provide an acceptable alternative to contemporaneous physical confirmations[16]. Rejection of the electronic equivalent would thus in all these cases be based on form rather than the substantive purposes of such documents - and this, in the light of the progressive undermining of form that has been occurring over a period of time, is a weak reason indeed.

There is of course also the *Electronic Transactions Bill* 1999 currently progressing through Parliament. This bill, which is based on the UNCITRAL Model Law on Electronic Commerce, is a key component of the Australian government's response to the demands of the on-line environment. This bill has the aim of providing a framework by means of which electronic communications will clearly be regarded as satisfying such legal requirements.

[16] Particularly when this is combined with the strong authentication and privacy maintaining features of cryptography.

Consensus

Offer

The basic rule is that the revocation of an offer is effective only when it has been brought to the attention of the offeree[17], and that the offer will lapse in any case in the absence of a reply from the offeree within a reasonable period of time[18]. Where the parties have chosen to transact by electronic means, however, it may not be clear when either party received messages. Using e-mail as an example, a message could be regarded as received:

- when it is received by the system operator, the system operator (Sysop);
- when it is forwarded to the client mailbox maintained by the Sysop; or
- when it is accessed and downloaded to the client computer.

The periods of time between each stage may be measured in some cases in terms of seconds (or fractions of seconds), and there may not be much in the distinction between them in many cases. In cases such as where a revocation has been sent immediately before an acceptance has been retrieved from the Sysop onto the offeror's computer, the distinction will become relevant as the sending of the revocation and the receipt of the acceptance may be separated by nanoseconds, and they may in fact have crossed within the system[19]. The issue may be determined in some cases by proof of the exact timing of each messages derived from system logs. This however is not a particularly practical solution, and given the possibility that such proof might not be conclusive anyway[20] it is likely that a pragmatic decision taking into account all the circumstances of the transaction will be made by a court called upon to decide such an issue[21]. In most cases it is now

---

[17] In other words the mere sending of the message will not suffice (a pragmatic rule based on paper transactions - see *Byrne v. Van Tienhoven* (1818) LR 5 CPD 344; [1874-80] All ER 1432) in contrast to the (postal) acceptance rule.

[18] *Ramsgate Victoria Hotel Co v. Montefiore* (1886) LR 1 Exch 109, also *Manchester Diocesan Council v. Commercial and General Investments Ltd* [1970] 1 WLR 241 at 248.

[19] This is assuming of course that the parties have not agreed in advance on the point at which messages will be deemed received and effective.

[20] Where they are simultaneous for instance. The logs also may or may not be admissible evidence in a court of law.

[21] See for example the comments of Lord Wilberforce on instantaneous modes of communication in Brinkibon *Ltd v. Stahag Stahl und Stahlwarenhandelsgesellschaft mbH* [1983] 2 AC 34 at 42 ("...many other variations may occur. No universal rule can cover

generally accepted in practice that a message is deemed delivered to its destination address when it has been delivered to the system where access may be had to the message by the addressee.

The instantaneous nature of electronic media at any rate may provide advantages to either party. On the one hand, it may benefit the eager offeree, standing by to immediately respond to an offer on its receipt, by making revocation practically impossible. On the other hand the offeror who has had a change of heart and wishes to revoke the offer would not be frustrated by the offeree avoiding physical contact or refusing to answer the telephone, but would be able to immediately forward that information to the offeree's fax number or e-mail address. The "retract" feature now available with some e-mail programs would be helpful in such situations, although it would be prudent to specifically revoke the offer, rather than merely retrieve it[22].

Acceptance

Where the method of communication is instantaneous, the interval between the transmission and receipt of the message of acceptance is very short indeed, and this may obscure the place or time of acceptance. In *Entores Ltd v. Miles Far East Corp*[23] the Court held that the place of acceptance of a telexed message was the location of the recipient telex machine, in other words the point of reception rather than the point of transmission. The circumstances were however regarded as being analogous to face to face or telephoned transactions, and the general rule requiring receipt of the acceptance by the offeror in such circumstances became the main determinant of the issue[24]. Implicit to the comparison between oral and telexed messages are the presumptions that: (a) the messages were truly instantaneous - i.e. that the recipient would receive them immediately, (b) the messages would be received by the addressee as soon as they were transmitted by the sender - i.e. that the recipient would also be the addressee or an agent

---

all such cases: they must be resolved by reference to the intentions of the parties, by sound business practice and in some cases by a judgment where the risks should lie...").

[22] Where the offer may not be withdrawn before the expiry of a certain period, for example because it is subject to an option or other agreement, its withdrawal will be ineffective, irrespective of whether the retrieval leaves no trace of its prior delivery. Where there is no evidence of its prior delivery, the addressor may escape liability merely because the addressee remains unaware that the offer was made.

[23] [1959] 2 QB 327. Also *Aviet v. Smith and Searies Pty Ltd* (1956) 73 WN (NSW) 274, *W.A Dewhurst v. Cawrse* [1960] VR 278, *Hampstead Meats Pty Ltd v. Emerson & Yates Pty Ltd* [1967] SASR 109.

[24] See also *Mendelson Zeller Co Inc v. T&C Providores Pty Ltd* [1981] 1 NSWLR 366.

of the addressee, (c) any failure of the message to get through to the addressee would most probably be due to some failure on the sender's part, and (d) that it was appropriate that the risk of non-receipt be placed on the sender.

These presumptions may not apply to other electronic means[25]. E-mail messages for example have the capacity to be instantaneous but may pass through several intermediaries before delivery to the addressee. Because of this, the message may be delayed during transmission or misrouted or lost even after receipt by the addressee's Sysop. The analogy therefore clearly breaks down in these circumstances, as the receipt of the message may not result in actual notification to the addressee. Possible options for the time of acceptance in such instances thus depend on the type of notice the Court would deem sufficient in the circumstances. If constructive notice would suffice, the offeree's duty of notification would be complete once the message is: (a) released and begins its journey upon the transmission route[26], (b) at a stage in its transmission where it is received by a Sysop connected with the addressee, though it has not yet been delivered to the addressee's mailbox maintained by the Sysop[27], or (c) delivered to the addressee's mailbox maintained by the Sysop. Increasingly, receipt of a message within the system from where the addressee may read the message, is being treated in practice as effective delivery.

---

[25] Per Lord Wilberforce in *Brinkibon Ltd v. Stahag Stahl und Stahlwarenhandelsgesellschaft mbH* [1983] 2 AC 34 at 42.

[26] In other words a gloss on the postal rule. A transmission that bounces (is unable to be delivered and is returned to the sender) would presumably be treated as the equivalent of a correctly stamped and addressed which nevertheless is returned to the sender unopened as undeliverable by the postal agency. On the corollary issue of whether an acceptance once sent can be revoked, the classic postal rule does not permit this as the contract is deemed binding once the acceptance has been released into the postal system - a phone call withdrawing the acceptance before delivery of the letter would thus be to no effect. In the absence of binding decisions on the point it has been suggested that as a matter of convenience (rather than logic) a choice may be possible to an offeree as it is possible (subject to the discretion of the Australian Post Office on the giving of satisfactory written reason) to recall and recover mail before it is delivered – see N Seddon, *Cheshire and Fifoot's Law of Contract*, 7th ed, Sydney, Butterworths, 1997 at 87. In the electronic context, depending on the time at which acceptance is deemed to be effected, it may be possible to overtake the message of acceptance in order to revoke it.

[27] This and the following three options do not regard the message as essentially instantaneous as they assume ability to pinpoint different stages of a transmission. All vicissitudes of the journey of the message of acceptance before the point of consensus would be at the risk of the offeree.

If in the alternative, actual notice was required, this would be effected either (a) when the message is downloaded by the mailbox maintained by the Sysop[28], or (b) when the message is actually read by the addressee[29].

One conclusion which may be drawn from the foregoing is that e-mail and similar messages fall within neither the postal rule or the instantaneous rule very neatly - in truth, matters pertinent to both tests are among the criteria the Court would consider in such cases[30]. Though it might seem at first glance that the instantaneous rule is being applied because acceptance is considered effective at the time of receipt rather than the time of transmission in all of the instances above except for one, the messages are not being treated as though they are truly instantaneous or analogous to oral statements as is the case with the instantaneous rule. A further gloss on this rule derives from the fact that the type of receipt involved is different from what was contemplated in *Entores* in that it is constructive rather than actual. The result of this is that agency issues[31] which were previously more germane to the postal rule, become directly relevant, and the resulting criteria summed up cannot be described as either test.

The above is but one of various difficulties stemming from the nature of the consensual model of contract[32]. Even the Court has noted that it may not always be possible to fit commercial arrangements within the benchmarks of classical contracts theory[33] even though they should be, and will be, held binding. Of course the facts may support the conclusion that no binding obligation has come into being between the parties in spite of lengthy negotiations, despite the desire of the Court to support bargains where possible. The Court in any event will

---

[28] The pragmatic assumption being made that this could only occur through the action of the addressee or agent of the addressee. Any circumstances making the situation otherwise would at any rate be regarded the responsibility of the addressee and not the concern of the sender.

[29] The most unlikely choice as this would be almost impossible to prove.

[30] These issues would not arise in the majority of cases because they would arise only where there had been a break in transmission or other system malfunction, or the message had bounced and had been rerouted back to the sender.

[31] Such as questions about which party is the principal of which intermediary.

[32] For a concise summary of the competing theories of contract law see Seddon, n26 at 17-45.

[33] Per McHugh JA in *Integrated Computer Services Pty Ltd v. Digital Equipment Corporation (Australia) Pty Ltd* NSW Court of Appeal (Unreported) 23 December 1988.

apply an objective test to the facts in order to determine the question in the light of all the circumstances of the case[34].

Genuine Consent

An issue relevant here is the seeming acceptance of an offer by the inadvertent selection of a menu option. Unless care is taken in the design of an options page, a prospective purchaser merely wishing to scroll through descriptive information examine may mistakenly depress an enabled acceptance button before any intention to purchase has been formed. The argument of lack of genuine consent would be available to the apparent purchaser, but its success might depend on how poorly the options page has been designed, and how often, or how likely it is that such a mistake would be made. Conceivably, a message immediately reporting the mistake and disclaiming any apparent intention to accept, and the non payment of the consideration contemplated by the transaction envisaged would strengthen the claim of no intention. Clickwrap agreements contested on this basis may also be objectionable on grounds similar to those applying to shrinkwrap licences.

Shrinkwrap Licences

This term is applied to a device software copyright owners use to try to protect their interests. It is often the case that retail suppliers, rather than copyright owners, market mass produced software to the general public, and that as a result, there is no direct transactional link between the copyright holder and eventual purchasers of the software[35]. The realities of commerce are such that sales would be hindered if prospective purchasers could purchase a copy only after they had read through the terms of a standard contract accompanying the software. Therefore, in an attempt to satisfy the requirement that notice of all terms be given before contract finalisation, the copyright owner arranges for the terms of the licence to use the software to be

---

[34] Where the facts are equivocal, the Court at its discretion may take subsequent actions or documents (entered into by the parties after the alleged contract) into account. The use of certain phrases during negotiations may have however enabled a party to avoid responsibility for assertions made which otherwise would be binding ("subject to contract", "without prejudice", "binding in honour only" etc are but a few examples).

[35] The copyright owner would be regarded as privy to the contract between the supplier and the end user only where the supplier had acted as agent for the copyright owner.

displayed[36] at a spot on the packaging where they would be impossible to miss before the package could be opened.

Although widely used, shrinkwrap licences are not favourably regarded by judges for several reasons[37]. First of all, the notice requirements are not satisfied as the terms are brought to the customer's attention too late for them to be a part of the contract. By the time the customer comes into contact with the terms[38] the contract will have come into being at the point of sale when the customer's payment or promise of payment was accepted by the supplier[39]. If those terms are to bind the customer therefore, they must form part of another contract that subsequently comes into being. This then raises the question of what has been purchased in the first transaction - the mere possession of a software package that may not be opened and used unless a further contract is entered into with the copyright owner? Or perhaps what was purchased was an opportunity - an opportunity to obtain from the software owner, permission to use the software now in the customer's possession? Both are unlikely, as no purchaser of software makes his/her purchase merely to own an unopened package. The court is more likely to find that terms for reasonable use were imputed into the purchase agreement - however this would still not be of much use to the copyright owner unless the supplier was inclined to enforce the observance of those limitations on the owner's behalf.

---

[36] Under transparent wrapping used to seal the package.

[37] In some instances, there has been resort to the enactment of legislation, in an attempt to resolve the doubtful status of shrinkwrap licences - see for example the *Software License Enforcement Act* 1984 of the state of Louisiana, USA. For more on shrink wrap licences generally see J FitzSimons, "Shrinkwrap Licences and the Law in Australia" (1989) 6 *Proceedings of the NSW Society for Computers and Law* 1, 5; C Miller, "Shrink wraps are Enforceable - an opinion" (1992) 8 *Computer Law and Practice* 52; DW Maher, "The Shrink-wrap Licence: Old Problem in a New Wrapper" (1987) 34 *Journal of the Copyright Society of the USA* 292; GP Smith, "Tear-Open Licences - Are They Enforceable in England?" (1986) *Computer Law and Practice* 128; MG Ryan, "Offers users Can't Refuse: Shrink-wrap Licence Agreements as Enforceable Adhesion Contracts" (1989) 10 *Cardozo Law Review* 2015; RH Sterm, "Shrink-wrap Licences of Mass marketed Software: Enforceable Contracts or Whistling in the Dark?" (1985) 11 *Rutgers Computer and Technology Law Journal* 51. See also the comments of the Federal Court Judges in *Autodesk Inc v. Dyason* in (1989) 15 IPR 1, 30-31, (1990) 18 IPR 109, 165-166.

[38] At home for example when the package is about to be opened. (It is unusual for this to occur at the place of purchase, not least because this might needlessly excite the store detectives on duty).

[39] See for example *Step-saver Data Systems Inc v. Wyse Technology* (1991) 939 F.2d 91. A principal/agent relationship between the copyright owner and supplier would not cure this defect - it would only mean that the premature contract was between the copyright owner and customer, rather than the supplier and customer.

Secondly, a shrinkwrap licence purports to constitute the act of opening the package[40] or the silence of the offeree an acceptance[41]. As the shrinkwrap licence in reality is no more than an offer made by the copyright owner to the end user, it must be accepted before it can have any effect. The terms of the shrinkwrap licence most often provide that the opening of the package will be deemed an acceptance of the shrink wrapped terms - however as rights of reasonable use (necessitating the opening of the package) would be imputed terms reasonably necessary for the business efficacy of the purchase contract, the argument that the opening of the package was to enable reasonable use as permitted under the contract of purchase rather than any imputed acceptance of the shrink wrapped terms, would be a successful one. Unless some other act or omission could be regarded as accepting conduct[42] therefore, acceptance of the terms would have to be inferred from the silence of the customer in failing to contact the copyright owner to expressly reject the offer[43]. It is true that a duty may be imposed on an offeree in some circumstances, to expressly reject an offer, and that the failure to do so will be construed as an act of omission sufficient to constitute an act of acceptance[44]. In those cases however, the offeree has a grace period, "a reasonable period of time", only after the elapse of which, would the omission to reply be construed as acceptance. The occurrence of a cause for dispute within this grace period would thus entitle the offeree to argue that no contract had come into being, as accepting conduct could not be imputed at that point in time. The categorisation of the failure to expressly reject the shrinkwrap terms as either mere silence, or accepting conduct, would thus depend on whether a reasonable period of time had elapsed at the time of opening the package. As this commonly occurs very shortly after purchase, it is likely that in many cases, the failure to reply on the part of the offeree would be construed as mere silence.

A third reason centers on the need for supporting consideration - identifying the consideration supporting the agreements involved in the shrinkwrap licence device may require fruitless mental contortions.

---

[40] As was permitted in cases such as *Brogden v. Metropolitan* Railway (1887) 2 App Cas 666 and *Empirnall Holdings v. Machon* (1988) 14 NSWLR 523.

[41] Which mode of acceptance is contrary to legal authority.

[42] Such as the completion and return of a registration form (the inclusion of which by the offeror could be taken as an implicit recognition of the inchoate nature (an offer) of the shrinkwrap terms).

[43] The imposition of an obligation to respond to an offer is also not something ordinarily approved of in such circumstances.

[44] Especially where some benefit provided by the offer has been taken advantage of by the offeree - see *Empirnall Holdings v. Machon* (1988) 14 NSWLR 523.

This depends on which device has been used in the circumstances to extend the restrictions of the shrinkwrap licence to the end user.

It may be that the device of implied terms may have been employed. For such terms to be of use to the copyright owner in the possession transaction[45], the supplier would have to have entered into that transaction as agent of the copyright owner[46]. The implication of such terms would also have to be reasonably necessary in the circumstances[47]. The purchase price supporting the entire agreement would obviously be regarded as supporting its constituent terms.

Another method would be to use the device of the collateral contract. The two main alternatives possible under this option would find either that the consideration: (a) for a subsequent restricted use contract had been provided by the customer entering into a prior collateral possession contract. Two different contracts with one party in common (the customer) would eventuate - one between the supplier and customer for the transfer of the possession of the software to the customer (a possession contract), and one between the copyright owner and customer under which the copyright owner agrees to grant limited user rights to the customer in exchange for the customer entering into the preceding possession contract[48] (a restricted use contract), or (b) for a subsequent possession contract had been provided by the customer entering into a prior collateral restricted use contract. Both contracts here would ostensibly involve the same parties (the customer and supplier) - one would involve the supplier acting as agent of the copyright owner granting limited user rights[49] to the customer; the other would also involve the supplier, but the supplier would be acting as an independent entity. Here the customer in consideration of the preceding restricted use contract, would agree to enter into a possession contract with the supplier. This however would not answer the question of what consideration had supported the prior restricted use contract to make it valid. Unless the restricted use

---

[45] The transaction by means of which possession of the software is transferred to the customer.

[46] See *International Harvester v. Carrigan's Hazeldene Pastoral Co* (1958) 100 CLR 644 at 653.

[47] Reasonably necessary in the circumstances, for the business efficacy of the transaction.

[48] This analysis would only make sense where the complaining party was the copyright owner, and the complaint being made was that the copyright owner had been induced to grant user rights to the customer. There would not be room for such a complaint at any rate unless the rights complained about were binding, and this is unlikely to be so where those rights were conferred by means of a shrinkwrap licence.

[49] These would have to be implicit as at that stage the shrinkwrapped terms would not have come to the attention of the customer.

agreement could be regarded not as a separate contract, but a part of the possession contract as above, it would be of no effect unless of course the customer had also paid or promised to pay something over and above the purchase price for the possession contract. Even where this was the case, it would still lead to difficulties. If the contracts were regarded as truly distinct, the possession contract would necessarily include a term of reasonable use, otherwise the customer would be agreeing to pay the supplier for the mere possession of the software without any right to open or use it - a most impractical and unlikely possibility. The subsequent restricted use contract would also have to be offering some enhancement[50] to the user rights granted otherwise it would in effect be an arrangement under which the customer pays the copyright owner to further restrict the previously obtained user rights - an even more unlikely possibility.

Another alternative would be to interpret the shrinkwrap licence as an independent contract. The offer embodied by the shrinkwrapped terms would require acceptance in some form by the customer. Where acceptance is held to have occurred as a result of an act on the customer's part, the same act may also be regarded as supporting executed consideration[51]. If acceptance on the other hand is imputed as a result of the customer's silence, the invoked duty to reject the offer within a reasonable time would need to also incorporate an implied promise to pay as executed consideration.

If it can be found that the shrinkwrapped terms were accepted by the offeree, it may be the case that remedies for defective software are validly restricted by its terms, and this would remain the case despite the fact that the customer was in effect presented with a take it or leave it ultimatum[52]. An extensive limitation clause excluding responsibility for the proper working of the software in those circumstances would bind the customer[53]. Exclusion of liability for negligence would be

---

[50] The provision of technical support or other services not otherwise available to the customer could be construed as such an enhancement. This however would depend on the facts of the case - the thrust of most shrinkwrapped terms tend to be to the effect that the customer is granted permission to do very little at all with the software.

[51] The return of a completed registration form would be an example of this. As consideration need not be adequate, but merely sufficient, the provision of the personal data in the filled form could be regarded as a thing of value to the copyright owner - for example for statistical, advertising, or target mailing purposes.

[52] "Either accept the terms (without an opportunity to check the software), or return the software immediately".

[53] Unless of course the clause had been rendered ineffective by a finding that it had been mitigated by fraud, there had been a total failure of consideration, or that the customer

permitted also, but only where this was clearly provided for by the wording of the clauses.

In those cases where the shrinkwrap licence is not regarded as a binding contractual document, it may still have an effect on the rights of the customer. A court may find that its wording was such as to affect the valid expectations of the customer. The type of restrictions that will be held to be a reasonable part of an implied restricted use clause are likely to be affected by the degree of familiarity the customer has or ought to have had with such terms. It is likely that the plea of complete ignorance of the nature of the transaction[54] would fall on deaf ears today. It is more likely that the court would have regard to the actual or reasonably expected exposure of the customer to such terms in determining what restrictions are reasonably to be implied into the customer's use of the software[55].

The digital equivalent of the shrinkwrap licence, the clickwrap licence[56], may not however involve such complexities. Firstly, the Internet permits direct communication between the original designer/producer of a product and its end user, undermining in one fell swoop the main premise of shrinkwrap licences - remoteness between the producer of a product and its end-user. It may be argued therefore that the clickwrap licence performs a different function than the shrinkwrap licence, namely providing an electronic form for the creation of immediate, direct, express contractual obligations. Then there is the fact that the contractual requirement of notice may be met, provided the digital "pages" or page options are designed with care. Designing the digital licence so that offeree cannot access the acceptance page without having first accessed the terms of the contract need not be a difficult task, and safeguards against the possibility of selecting or sending acceptance options in error would further strengthen such licences. The argument about silence as purported acceptance would also be irrelevant in many cases, as there would be the affirmative action (conduct) of the selection of contract acceptance options.

---

had transacted as a consumer as certain terms implied by statute cannot be excluded from consumer contracts.

[54] For example that there was complete ignorance on the customer's part that the possession transaction was not an outright sale but a mere license.

[55] See for example *North American System Shops v. King* (1989) 45 BLR 242 (ABQB).

[56] The agreement intended to come into being through the selection of menu options signifying consent to terms displayed within a (digital) document accessed and executed via the Internet.

The nature of the digital transaction is in any case significantly different from physically conducted ones and the process of transacting is reversed. Unlike shrinkwraps where the terms of the licence are typically brought to the attention of the purchaser after the goods have been purchased and transported away from the place of sale, the subject of clickwraps need not be available to the prospective purchaser without at least constructive notice of the terms, as the accessing of all the relevant terms can easily be made a condition precedent to its delivery. Unlike the case of shrinkwraps, this is a practically feasible option. In contrast to shrinkwraps therefore, clickwrap licences would in most cases be easily effective.

"Goods" or "Services"?

The terms implied into a computer related transaction[57] will vary[58] according to whether the subject matter of the transaction is characterised in law as "goods"[59], "services" [60]or a mixture of both.

Statutory definitions of these terms tend to be inclusive[61] and as such are of limited help when a dispute centres on the distinctions between the two. In practice the differences between both are not always clear cut, therefore one must resort to supplementary distinguishing devices. One such device is the "substance of the contract" test[62]. This looks at what the overriding purpose of the transaction is. If it is for the sale (or other transfer) of an article the transaction is regarded as one for the transfer of goods. If on the other hand, the main purpose of the transaction is the procurement of the exercise of skill and labour by a party, the end product of such exercise

---

[57] Under the common law or under legislation such as the Trade Practices or Sale of Goods Acts.

[58] The analysis adopted in *Saphena Computing v. Allied Collection Agencies Ltd* [1995] FSR 616 (3 May 1988 CA), to the effect that the distinction didn't really matter as the same obligations would apply in any case is suspect, and certainly does not apply to Australia.

[59] Or a "product".

[60] Or "work & materials".

[61] See for example s4 *Trade Practices Act* 1974 (Cth) which provides that "'goods' includes.... vehicles....animals.... minerals.... tree.... crops.... gas and electricity" and also that "'services' includes any rights (including rights in relation to, and interests in, real or personal property), benefits, privileges or facilities that are...provided, granted or conferred in trade or commerce, and without limiting the generality of the foregoing, includes....".

[62] This test was strongly criticised by Fullagar J in *Deta Nominees v. Viscount Plastic Products Pty Ltd* [1979] VR 167 at 181 as being unworkable and illogical.

of skill being regarded as ancillary, it is regarded a transaction for the provision of services[63].

This test was adopted in *Toby Construction Pty Ltd v. Computer Bar (Sales) Pty Ltd*[64]. The plaintiff was suing the defendant for damages for the supply of a defective computer system. The main matter in issue was whether the statutory warranties applicable to agreements for the sale of goods under the NSW *Sale of Goods Act* applied to their transaction. The transaction had envisaged that three hardware items, two software items, technical support, upgrades, staff training, installation and a few other services would be provided by the defendant[65]. The defendant contended that the transaction was not one for the sale of goods but rather one for work to be done and the transfer of incidental materials and possibly intellectual property rights[66], or alternatively, that warranties for the sale of goods were irrelevant to the dispute because the subject agreement was divisible and the relevant part related to software only[67]. The court decided that the agreement was one for the sale of goods for several reasons[68]: (a) the contract had envisaged and resulted in the transfer of identifiable physical property albeit with the supply of intangibles also, and the system, although once the result of much research and work, was really an off-the-shelf system and mass produced[69]; (b) the application of "the substance of the contract" test in the circumstances required the evaluation of all the features of the subject matter of the transaction, and the provisions employed[70] to effect its transfer; (c) it would be too simplistic to categorise the transactions as one for the sale of "goods"

---

[63] See *Lee v. Griffin* (11861) 1 B & S 272; *Robinson v. Graves* [1935] 1 KB 579, applied in *Brooks Robinson Pty Ltd v. Rothfield* [1951] VLR 405 at 407.

[64] [1983] 2 NSWLR 48.

[65] The total contract price was $14,390 ($12,230 for the hardware, $2160 for the software; both were off-the-shelf packages).

[66] In other words that the main purpose of the transaction was the design, production and transfer of the software command module without which the hardware would not function, making it one for the supply of skill and labour.

[67] Implicit to this argument was the assumption that agreements involving software alone could not be categorised as "goods".

[68] In reaching this decision, the court had reference to North American authorities where there had been the same express or implicit finding (*Triangle Underwriters Inc v. Honeywell Inc* 457 F Supp 765; *Chatlos Systems Inc v. National Cash Register Corporation* 479 F (Supp) 738; *Public Utilities Commission for City of Waterloo v. Burroughs Business Machines Ltd* (1973) 34 DLR (3d) 320; *Burroughs Business Machines Ltd v. Feed-Rite Mills* (1962) Ltd 42 DLR (3rd) 303). The court dismissed as too simplistic an approach under which the fact that a certain element represented the greater amount of the transaction price.

[69] "There can be no comparison with a one-off painting. Rather it is the comparison with a mass produced print of a painting...." per Rogers J at 51.

[70] Relating to various ingredients such as the price, the nature of the material to be supplied, installation terms, the work the system was designed to perform.

merely because the bulk of the cost related to the hardware; and (d) it would also be simplistic to find that the transaction was one for the transfer of goods merely because the hardware would not work without the supplied software. The substance of the agreement in issue was in truth for the sale of physical property, the fact that that physical property was dependent on intangible software for its operation, would not prevent it from being such.

The judge did not rule on the question of whether software alone could be categorised as "goods" although he was careful to scotch any possibilities of the instant judgement being used as such an authority[71]. The preponderance of overseas authorities suggest that such transactions should be categorised as for "goods"[72] although there have also been decisions to the contrary[73]. In a relatively recent case, the Federal Court adopted the minority approach. In *Caslec Industries Pty Ltd v. Windhover Data Systems Pty Ltd*[74] the transaction in issue had envisaged the purchase of off-the-shelf business management software by the applicant from the respondent, the respondent installing the software and also providing staff training, enhancements, and other associated services. However, the software was found to be defective and the applicant eventually abandoned the transaction. The applicant then sued for damages, relying inter alia on breaches of warranties implied into contracts for the provision of services[75]. Although the applicant had purchased new hardware upon which the software was to operate at the same time as entering into the instant transactions, it had been purchased from a third party – therefore the applicant's claims against the respondent were limited to the software deficiencies. In awarding judgement for the applicant, the court found that: (a) that the sale of software should not be treated relevantly as a

---

[71] At 54 "I do not wish it to be thought that I am of the view that software by itself may not be "goods". The authority which is usually quoted for the affirmative answer is *Clements Auto Co v. The Service Bureau Corp* (1971) 444 F (2d) 169, a decision of the Court of Appeals for the 8th Circuit. However, reference to that decision does not bear out in full the proposition for which it is cited..... the point has never been squarely decided." See also at 54 "The questions arising here are obviously of considerable importance to the computer industry, and I think it is appropriate that those who attend to matters of law reform should consider whether or not legislative action is required to ensure that the matter is put beyond argument. As computers and programs become more accessible to the ordinary consumer, it seems appropriate in the public interest that the question which heretofore has troubled only commercial purchasers should be clarified".

[72] *St Albans' C&D Council v. International Computers* [1995] FSR 688 and *Schroeders Inc v. Hogan* 137 Misc 2d 738 (1987).

[73] *Data Processing Services Inc v. Smith Oil Corporation* 492 NE 2d 314 (1986).

[74] Unreported, Federal Court of Australia, NSW Division, 13 August 1992.

[75] Sections 70, 71, and 74(2) of the *Trade Practices Act* 1974.

sale of goods; (b) that the essence of the transaction was for the supply of off-the-shelf software and incidental services such as staff training, and enhancements, and (c) that the transaction related to a contract for the provision of services.

In arriving at the finding that the transactions solely for the sale of software ought not to be regarded as for the sale of goods, Gummow J referred to his earlier joint decision in *ASX Operations Pty Ltd v. Pont Data Australia Pty Ltd*[76]. There the question of whether delivered electronic data was "goods" or "services" had arisen at the trial stage, and the trial judge noting that the statutory definition of goods involved included electricity, had ruled that electronically delivered financial data as supplied by the defendants were goods[77]. In response to this it was remarked in the joint judgement that:

> "In our view.... it does not follow from the inclusion of electricity in the definition that it should be read as if there was a further inclusion, by way of extension of the ordinary meaning of "goods", so as to draw within the definition encoded electrical signals. At the heart of the three agreements is the provision by ASXO to the subscriber of stock exchange information; this is provided by electronic means, but one could not properly characterise the subscribers as purchasers of electricity, and therefore of goods, within the sense of s. 49.... We should add that in *Toby Constructions Products Pty Ltd v. Computa Bar (Sales) Pty Ltd* (1983) 2 NSWLR 48, Rogers J held that a sale of a computer system, comprising both hardware and software, was a sale of "goods" within the meaning both of the *Sale of Goods Act* 1923 (NSW) and the warranties implied by Part V of the *TP* Act. His Honour said (supra at 54), with reference to United States authorities, that

---

[76] *(No 1)* 19 IPR 323 (1991).

[77] ".... [the party] supplies to its subscribers a series of encoded electrical impulses supplies to its subscribers a series of encoded electrical impulses which are capable of reception and interpretation by the subscribers' computers. It is doubtful whether anyone hearing the word "goods", in normal parlance, would readily think of electrical impulses. The word generally refers to tangible and visible objects; although it is notable that both the Oxford English Dictionary and the Macquarie Dictionary define "goods" or "goods and chattels" as referring merely to "movable property", without further limitation. But whatever the ordinary meaning of the word, there is here a statutory definition that defines the word - in an inclusive, rather than exclusive, manner - so as to include electricity. It cannot, I think, be doubted that, as Parliament intended the word "goods" to be understood as including electricity, it also intended it to include encoded electrical impulses" *ASX Operations Pty Ltd v Pont Data Australia Pty Ltd (No 1)* 19 IPR 323 at 330 (1991).

> he did not wish it to be thought he was of the view that software by itself may not be "goods". *This is a question which is left open after the present appeal, which, as will be apparent, has decided a narrower point."*[78]

Although the intended effect of this decision was to leave the question open, Gummow J considered the facts of *Caslec* as providing an opportunity to address the issue squarely. Unfortunately, there was not any detailed analysis of the issue in the case. In response to contentions by counsel for *Caslec* that *ASX Operations Pty Ltd* supported the proposition that "the sale of software should not be treated relevantly as a sale of goods", and further, that the instant transaction with Caslec was essentially an agreement for the provision of an off-the-shelf package and incidental services, Gummow J merely accepted those contentions and without more ruled that the relevant warranties relating to contracts for the provision of services applied to the facts. Though weakened perhaps by the lack of detailed analysis of the issue, it thus stands as authority for the proposition that a transaction relating solely to the transfer of software[79] and the provision of incidental services is one for services. This may be contrasted with *St Albans C&D Council v. International Computers* where it was opined at first instance that software was "probably" goods[80].

On this analysis a transaction for the sale or lease of hardware"[81], systems integration, (OEM or VAR) contracts or a turnkey computer system[82] would be considered as relating to "goods" while those for the design and supply of bespoke or customised software, the provision of off-the-shelf software, or the installation of software and the provision of associated services would be categorised as for "services".

It is worthy of note that this issue has sometimes been resolved by treating the contract as an innominate one - depending on the

---

[78] Emphasis added.

[79] Where the software is customised or bespoke, that affinity with the provision of services is increased.

[80] "Software is a good, it can't be anything else...." per Scott Baker J. See [1995] FSR 686, [1996] 4 All ER 481. On appeal, it was commented that while a disk with defective software constituted goods for the purposes of the sale of goods legislation, a program directly transferred onto a computer by a supplier without the supply of the program on a floppy disk, would not be a supply of goods.

[81] Clearly this would often involve the provision of incidental services.

[82] A complete system - complete in the sense that it would include both hardware (for example a monitor, CPU, hard and floppy drives, a printer, a CD player) and software (operating and applications).

circumstances it may be determined by the implication of terms at common law, the interpretation of the actual terms, or the specific categorisation of the subject matter where possible[83].

Electronic Financial Transactions

It has been acknowledged above that the Internet provides the backbone for electronic commerce. Of increasing importance to the growth and development of electronic commerce are electronic financial transactions, of which there are now several varieties. Abstract electronic financial transactions are of particular interest, particularly Stored Value Card (SVC) systems and digital cash.

Developing Varieties and Choice

The increasing role of technology has produced significant differences in the types of payments systems that are available today. This becomes more evident when the different systems are categorised into "generations" and compared on that basis.

The evolution of payment methods over the centuries may be described in terms of nine different generations that may be sub-divided into four main groups:

- the *objects-as-money*[84] group consisting of:
- the first generation - trade by barter
- the second generation - trade with valuable objects
- the *currency-as-money* group consisting of:
- the third generation - coins
- the fourth generation - paper notes
- the *claims-as-money* group consisting of:
- the fifth generation - deposit accounts
- the sixth generation - "plastic money"
- the seventh generation - electronic payments (EPs) and electronic fund transfers (EFTs)[85]

---

[83] See *Saphena Computing Ltd v. Allied Collection Agencies Ltd* [1995] FSR 616; *Beta Computers (Europe) Ltd v. Adobe Systems Ltd* 1996 SLT 604; 1996 SCLR 587. See also HL MacQueen, "Software Transactions and Contract Law" in L Edwards and C Waelde, *Law and the Internet: Regulating Cyberspace*, Oxford, Hart Publishing, 1997 at 124-128.

[84] For the purposes of identifying the four main generation groups, the word "money" is used descriptively in a very loose sense.

- the *electronic-impulses-as-money* group:
- the eight generation - smart cards[86]
- the ninth generation - digital coins

Though all of the generations above are payment methods and are all part of a single evolutionary continuum, they are not all properly described as money - depending on the perspective adopted, some may be more accurately described as a means of payment[87].

Stored Value Card (SVC) Systems

These are based on financial applications of smart card technology that involve the card operating as a storage receptacle and transacting device for financial data. Wholly electronic financial transaction systems may be distinguished according to whether they involve the transfer of account balances, incorporate electronic cheques, utilise secure value counters, or are token based[88]. It is however those systems where the smart card is used to provide a secure counter of value, or where the card is used to store digital value in the form of transferable denominated tokens, that are of present interest.

In both cases the smart card functions as a storage receptacle of financially related data, however the data is composed, processed, and transferred in significantly different ways - secure counter systems utilise electronic evidence of prepaid value which is mostly transferred inflexibly, token based systems on the other hand revolve around denominated electronic value that is transferable and usually capable of storage in alternate media. Where the smart card stores electronic prepaid value, it functions as a stored value card (SVC), storing

---

[85] The sixth and seventh generations overlap somewhat in that plastic cards (both credit and debit) are used to effect EFTs, and even manual credit card transactions now involve automated authorisation procedures.

[86] The smart card may fall within either the third or fourth groups, depending on whether it is used as just another (albeit vastly improved) form of plastic money, or as a means of storing and exchanging electronic impulses as value inter partes.

[87] Although money is one of several means of effecting payment, it is not the case that all means of payment are money. For more on this topic, O Akindemowo, "The Fading Rustle, Chink and Jingle: Electronic Value and the Concept of Money" (1998) 21(2) *UNSWLJ* 466. See also G Tucker, "Some Legal Issues Relating to Digital Cash on the Information Highway" (1995) 6(2) *Journal of Law and Information Science* 46, and generally chapter three of O Akindemowo, *Information Technology Law in Australia*, Sydney, LBC Information Services, 1999.

[88] See A Furche and G Wrightson, *Computer Money*, Heidelberg, dpunkt, 1996 at 25-33.

electronic evidence of prepaid value, and is often referred to as an electronic purse.

Electronic purse systems are presently hardware related, while digital cash systems tend to be software based. This has an impact on the form and expression of digital data/value incorporated (inflexible stored counter, or denominated coins), the memory capacity required, the method by which the data is amended or transferred (via the Internet, by telephone, through portable terminals or wallets[89], by EFTPOS, through ATMs), and whether this may be done by remote exchange or requires the physical debiting of the card balance. As technology permits development of cheaper cards with increased storage capacity and security features, it is likely that both functions will become interchangeable or that the distinctions between them will be significantly diminished[90].

Underlying Legal Transactions

The transaction will create a debt that is owed by the card issuer to the merchant because the merchant in effect grants credit to cardholders on the basis of previous arrangements between the card issuer and merchant. As is the case with credit cards, it is most likely that the debt will be regarded as extinguished between the cardholder and merchant, but not between the card issuer and merchant[91]. As the value was prepaid by the cardholder, that party would not owe the card issuer a debt for the transaction.

---

[89] An "electronic wallet" is a device that enables cardholders to transfer or exchange stored data/value between cards without the need to log onto the card issuer's system. Contactless cards contain an antenna that permit them to use radio frequencies to transmit data once the holder in within the general vicinity of a terminal; contact smart cards must be placed within a terminal with a reading device before a transaction may take place.

[90] Although both forms are presently supported by pre-paid value, it is conceivable that digital cash may eventually circulate so freely as to operate as currency without it necessarily being declared legal tender, while SVC functions continue to relate to money deposit account value instructions. For more on Smart Cards and Money generally, see Centre for Electronic Commerce (for the Australian Commission for the Future), *Smart Cards and the Future of Your Money*, (Melbourne 1996) especially chapters 2, 5 and 7.

[91] Although of course depending on the structure and speed of card-issuer/merchant communications, this debt may be extinguished within very short periods of times.

Digital Cash

A variety of terms invoking associations with money are used to describe the subjects of an even more radical type of electronic transaction. Term such as "electronic money", "digital currency", "cybermoney" are used in different ways, sometimes to collectively refer to more than one generation of payment methods[92]. The term digital cash has been chosen here to refer to particular payment methods in which electronic impulses are dealt with as money. They are distinguished for the purposes of this analysis from current electronic purse transactions though they are closely related, and likely to become indistinguishable in some applications in the future[93].

The term "digital cash" is used here to refer to those electronic impulses that are employed as more than instructions for the subsequent debiting/crediting of an account, or evidence bringing pre-agreed credit agreements into operation. The arrangement of digital cash systems is such that they envisage the exchange of electric impulses as the end, and not merely the means of the transaction. Consequently in some system configurations the digital data is treated as value, rather than instructions about value[94]. Although present protocols presently incorporate single use tokens and occasional or eventual references to an issuing/validating financial institution, digital cash transactions forecast the eventual exchange of such value without the need for such reference. Protocols incorporating multiple use tokens will thus permit peer-to-peer transactions. In so far as transactions of this type are the most likely predecessor of freely

---

[92] See International Congress of Comparative Law, M Stathopoulos (ed), *Modern Techniques for Financial Transactions and their Effects on Currency: General and National Reports*, Boston, Kluwer Law International, 1995 at 10, 11 for example where the term "electronic money" is used to refer to both electronic payments such as EFTPOS, and smart card transfers, and at 12 "...the descriptions 'plastic money' or 'electronic money' suggesting currency of another kind are not exact...by the expression 'electronic money...all that is meant is payments effected by use of electronic methods from already existent claim money". See also the *Financial System Inquiry Final Report*, Canberra, AGPS, 1997 where electronic money is used to refer to digital cash, electronic purses and credit card cyberpayment - see at 103 of the Report. Cf A Tyree, *Digital Cash*, Sydney, Butterworths, 1997 which examines commerce in cyberspace generally, but restricts use of the term digital cash to digital tokens.

[93] For an interesting comparative analysis of privacy and transactional quality properties of conventional payment facilities and digital cash, see LJ Camp, M Sirbu and JD Tygar, *Token and Notational Money in Electronic Commerce*, 1995 available from http://www.ini.cmu.edu/netbill/pubs/camp/usenix.html

[94] This will be especially so where only the originating issue of the value, but not subsequent exchanges of the data are associated with a pre-payment. It is likely however that the exchanged data will retain a redemptive value.

circulating value, it is submitted that they are presently the most deserving of any of the above terms evoking the function of money.

It is probable that digital currency, if and when it eventuates, will be based on multiple use token-based systems. The portability and/or (in)violability of the media upon which such value could be stored would however also raise many security issues[95] as would the possible location of substantial amounts of value outside conventional financial domains.

Underlying Legal Transactions

Unlike electronic purses, the transaction between the cardholder and payee is not a credit transaction because the payee immediately receives value in the form of a token that may either be redeemable at the option of the payee, or non-redeemable, having a face value enabling it to be used as a form of currency. In such a case, the transaction may result in final payment where completion of the transaction between the holder and payee is not dependent on clearing or other authorisation procedures. Relations between the issuer of the value and the holder of the value will become more remote in that the issue may be based on a pre-payment by the original holder of the token, to the issuer, however subsequent holders will possess the electronic value as the result of a transaction with a previous holder of the value rather than the issuer. Where the token has a face value only and operates a non-redeemable currency, its transfer will satisfy the debt obligation created between a holder and payee without creating corresponding debt obligations between the issuer and payee, nor holder and issuer. Even in cases where the token is redeemable, it is arguable that it will represent an obligation of the issuer to exchange the token, on the demand of any holder, for monetary value, rather than satisfy the debt created by a sale transaction.

Strained Legal Definitions: Is Digital Cash "Money"?

It is obvious that payment transactions are becoming increasingly abstract. From its origins as a thing in possession, money evolved to become the tangible embodiment of a thing in action and it now

[95] Including risks posed by (unauthorised duplication, multiple spending) and posed to (robbery, irrecoverable destruction of storage media with value) the holder of value.

progresses towards becoming the intangible embodiment of a thing in action.

The potential for abstract elements is introduced where the exercising of rights apart from the possession of an object becomes an option within a transactions framework. This potential is significantly utilised by digital cash systems where transactions and the concept of value have become less tangible and more abstract. In some instances this results in the convergence of the medium of payment and the payment value making it difficult to distinguish the two. In such cases the digital data instructing the transfer of value from a transferor-payer to a transferee-payee itself in effect is treated as value to the benefit of the transferee-payee. The security and ease of such electronic transactions, their irrevocability nature and speed and other such features, are likely to encourage the increased use and acceptance of such transfers. As they begin to be used in large numbers, no doubt those espousing wider definitions of money will unhesitatingly identify such transfers as money[96].

Regulatory Triggers

Digital cash introduces consequences which supervisors of the financial system may justifiably be concerned about[97]. From one perspective, supervisors of the financial system may be seen to be less concerned with regulating money per se, than with ensuring the safety and stability of the payments system. Controls on money are of course central to such an objective - the impact of other catalysts or phenomena on the payment system however, must also be taken into account if supervisory arrangements for the financial system are to be effective. Thus, the issue is really one of degree - at what point does regulatory scrutiny or control become unwarranted or begin to resemble totalitarianism[98]?

---

[96] For more on this topic, see Akindemowo, *Information Technology Law in Australia*, n87.

[97] See for example the *Financial System Inquiry Final Report*, n92 at 236, 237, and chapters 7, 9 generally.

[98] For more on regulatory issues raised by digital cash, see B Lee and O Longe-Akindemowo, "Regulatory Issues in Electronic Money: A Legal-Economics Analysis", (1998) *1 Netnomics* 53-70 which is available at http://ns.baltzer.nl/netnomics/netnomics.html

Certain features of digital cash may seen predisposed to arouse the attention of regulators, especially when certain questions are asked: (a) technical distinctions aside, does it have the capacity to function or have similar effects as money? The fact that digital cash will enable ready transfers or access to value will be significant here, as will the fact that it may eventually become a digital currency; (b) is it conceivable that public confidence in the payments system, or in the financial system generally, may be detrimentally affected? Could the issue of prudentially unsound digital cash, culminating in the collapse of an issuer, possibly trigger public panic causing a domino effect reminiscent of past bank failures? (c) could national financial sovereignty be threatened in anyway by the ease of value transfers across geographical borders the technology permits? Is foreign or criminal control of large value trans-border transfers feasible? (d) what percentage of value in the financial system is likely to be in the form of digital cash in the foreseeable future?[99]; (e) are any consumer protection matters already entrusted to regulators raised by digital cash systems[100]? The impact of the use of misleading terms[101] on levels of use, and the potential created for extensive invasions of privacy would be relevant here.

In the early stages of the development of this technology which is still evolving, it is also a possibility that the exaggeration of, or the placing of undue emphasis on the likelihood of certain risks[102] may also be used as the justification for regulation which hindsight may prove to have been unwarranted. The nature of the technology is such however that it is being recognised that the possibilities for international cooperation, and possibly harmonisation, must be taken into account in the development of relevant national regulatory frameworks[103]. Issues such as these were taken into account by the

---

[99] Some governments such as Singapore's are reported to have the aim of converting their national payment systems into digital ones by the year 2020 – *Financial System Inquiry Final Report* (Wallis Report), n92 at 106.

[100] See for example the *Financial System Inquiry Final Report*, n92 at 291.

[101] Such as deliberately evocative descriptions of systems as providing "money" or "anonymous" transactions where this is not in fact the case. An example is the experience of the developers of Mondex who were forced to stop describing their electronic purse system as anonymous - see http://www.privacy.org/pi/issues/mondex/mondex-release.html.

[102] Which in fact may be technically impossible, though not manifestly so to those who are not technical specialists in the field - see A Furche and G Wrightson, n88 at 83, 84. Some advocates of regulators have suggested, in contrast, that some participants in fact desire regulation, as this will endow a certain amount of credibility upon their operations.

[103] See for example the *Financial System Inquiry Final Report*, n92 at 292 - 294.

Attorney-General's Electronic Commerce Expert Group 1997[104] in considering what form of regulatory framework to recommend for adoption in Australia[105].

Restrictions on Who May Issue Digital Cash

The answer to the question of who may issue digital cash, and electronic purses in open systems will depend, generally speaking, on the approach adopted by the central regulator.

The desire to maintain an environment encouraging and facilitating innovation may be strong. The historical development of the system may have led to a situation where NBFIs and possibly other possible participants are permitted a relatively broad scope of activity in comparison to other jurisdictions. The existence and applicability of a variety of regulatory controls, legislative and otherwise to the financially related activities such entities may further support the taking of such a position, as may a trend towards historical influential deregulation policy. The belief that this permits desirable flexibility while allowing for retrospective change of position if necessary may also be influential.

This type of reasoning has been influential in Australia[106]. Co-regulation, for example, was the preferred option of the Wallis Committee, and the central philosophy of the *Payments Systems (Regulation) Act* 1998 (Cth) passed in response to the recommendations of the Wallis Committee[107]. The Committee was also of the view that

---

[104] See for example the Terms of Reference of the Electronic Commerce Expert Group, and its Issues Paper No.1 available from http://law.gov.au/aghome/advisory/eceg, See also the final report: *Electronic Commerce: Building the Legal Framework*, Canberra, Attorney General's Department, 1998. Available from http://law.gov.au/aghome/advisory/eceg

[105] The Electronic Commerce Expert Group recommended that adoption of a minimalist regulatory model requiring the enactment of legislation in limited circumstances only, expressed in technology neutral terms - see their Final Report (Attorney General's Department, 1998) at chapter three, and their recommendations in the Executive Summary, n104.

[106] See the Overview of the Wallis Committee's Final Report - *Financial System Inquiry Final Report*, n92 particularly at 11-15.

[107] See the summary of key measures proposed in para. 4.1 of the Explanatory Memorandum to the *Payment Systems (Regulation) Bill* 1998. See generally, the Government's Response to the Financial System Inquiry, including the associated Bills, explanatory memoranda, and press releases at http://www.treasury.gov.au/publications /GovResponseFSI/Default.asp

the issue of electronic value need not be limited to licensed deposit taking institutions only[108].

The Australian approach falls somewhere between that of the United States, where there has been a clear reluctance to possibly short-circuit innovation or squelch competition by prematurely adopting regulation[109]and that of European states such as Germany where a more pro-active approach has been adopted. The retaining of extensive central control has been stated as a clear objective in such jurisdictions, and the prohibition of the issue of such value by entities other than banks, is a clearly emerging policy in such jurisdictions[110].

The Reserve Bank has now, in any event, been given wide powers to regulate such payment systems[111] under the *Payments Systems (Regulation) Act* 1998 (Cth). This includes the power to designate particular payment systems as being subject to its direction[112], as well as the power to impose and enforce access regimes, make standards for, and arbitrate disputes relating to systems so designated[113]. The Act does not envisage participation in payment systems other than by corporations, as a payment systems participant is defined as a constitutional corporation that is either a participant in the system in accordance with the rules governing the operation of the system, or an

---

[108] It was however considered prudent that non licensed participants in open systems be required to hold collateral against unsettled claims, or meet other requirements as determined by the PSB. Participation in closed systems was considered to pose little systemic risk, and deemed appropriately regulated under existing corporations law and consumer protection legislation. It was however further recommended that such systems be subject to an industry Code of Conduct overseen by the CFSC - see *Financial System Inquiry Final Report*, n92 at chapter 9, especially at 401-404.

[109] See for the example the remarks of Alan Greenspan, Chairman of the US Federal Reserve Board made at the US Treasury Conference on *Electronic Money and Banking: The Role of Government*, Washington DC (September 19, 1996) available at http://www.bog.frb.fed.us/BOARDDOCS/SPEECHES

[110] See Working Group on EU Payment Systems, *Report to the Council of the European Monetary Institute on Prepaid Cards* (May 1994) – see http://www.systemics.com/docs/papers/EU_prepaid_cards.html. For a critique of the position taken by the Working Group, see I Grigg, *Critique on the 1994 EU Report on Prepaid Cards*, available from http://www.systemics.com/docs/papers/1994_critique.html

[111] Defined as funds transfer systems facilitating the circulation of money including any instruments and procedures relating to such systems - see the definitions section, s7, of the *Payments Systems (Regulation) Act* 1998 (Cth).

[112] Where this is in the public interest - see s11(1) *Payments Systems (Regulation) Act* 1998 (Cth). It has been estimated that a sizeable number of payment systems will not be so designated - see para. 4.1 of the *Explanatory Memorandum to the Payment Systems (Regulation) Bill* 1998. The designation, which will be by a notice published in the government Gazette, will be effective until revoked - s11(1) - 11(3) of the Act.

[113] See ss12-21 *Payment Systems (Regulation) Act* 1998 (Cth).

administrator of the system[114]. This is of course in line with the philosophy of the *Banking Act* 1959 (Cth) under which it is provided that only corporate bodies may be licensed to carry on the general business of banking[115].

The term "bank" is also now defined in terms of the concept of an Authorised Deposit-taking Institution (ADI), which is further defined as a body corporate in relation to which an authority to carry on banking business is in force[116]. Banking business has been redefined to include "a business consisting of banking according to paragraph 51(xii) of the Constitution, or business carried on by a corporation to which paragraph 51(xx) of the Constitution applies which also consists of both the taking of money on deposit (otherwise than as part-payment for identified goods or services) and the making of advances of money, or other financial activities prescribed by regulations." As the operation of SVC systems does not necessarily involve the making of advances, it may be argued for this reason that the operation of an SVC facility will not constitute the carrying on of banking business for the purposes of this section. Regulations enacted pursuant to the section may however provide otherwise[117]. Where a digital cash facility requires the initial purchase of digital cash to be based on conventional cash or conventional account based payments, the seller of the digital credit/payee of the conventional payment will be involved in the taking of deposits. It is possible however that the subsequent circulation of the digital cash will be accomplished on the basis of wholly digital value exchanges - the operator of such a system would arguably be able to escape regulation as an ADI where the initial deposits are made to another party participating as a separate entity.

The Reserve Bank is also given increased oversight and regulatory control over payment facilities including travellers' cheques, SVCs and digital cash, particularly "to ensure that the holders of the stored value behind purchased payment facilities operate in such a manner as to provide security to the store of value"[118]. Holders of the stored value backing purchased payment facilities must now be either an ADI or an

---

[114] See s7 *Payment Systems (Regulation) Act* 1998 (Cth).

[115] See ss7 & 9 *Banking Act* 1959 (Cth).

[116] See s5 *Banking Act* 1959 (Cth) as amended by the *Financial Sector Reform (Consequential Amendments) Act* 1998 (Cth).

[117] See A Beatty, M Aubrey & R Bollen, "E-Payments and Australian Regulation" (1998) 21(2) *UNSWLJ* 489 on the new regulatory framework in Australia.

[118] See para. 4.1 of the *Explanatory Memorandum to the Payment Systems (Regulation) Bill* 1998. Also ss22-25 *Payment Systems (Regulation) Act* 1998 (Cth).

entity in possession of an authority or exemption issued by the Reserve Bank[119]. A purchased payment facility is defined in the Act as:

> a facility (other than cash) in relation to which the following conditions are satisfied:
>
> (a) the facility is purchased by a person from another person; and
>
> (b) the facility is able to be used as a means of making payments up to the amount that, from time to time, is available for use under the conditions applying to the facility; and
>
> (c) those payments are to be made by the provider of the facility or by a person acting under an arrangement with the provider (rather than the use of the facility).

The holder of the stored value in relation to such facilities is defined as the person who is to make payments under (c)[120].

The holding of the stored value of purchased payment facilities by entities other than ADIs is now a criminal offence where the entity possesses neither an authority or an exemption issued by the Reserve Bank. The offence carries a fine of 200 penalty units, although a court under s.4B(3) of the *Crimes Act* 1914 (Cth) may impose a fine of up to five times that penalty[121].

Computer Crimes using the Internet

Certain legal conceptions and policies made the criminalisation of computer abuse problematic historically. Those problems, in many cases have now been overcome by the enactment, amendment or expansive interpretation of legislation.

Wrongful Access and Damaging Data

Hacking into remote computers with or without the alteration or impairment of data is a federal offence under the *Crimes Act* 1914. The

---

[119] See s22 *Payment Systems (Regulation) Act* 1998 (Cth). See also ss23-25 which deal with applications and grants of authority, and exemptions.
[120] See s9 *Payment Systems (Regulation) Act* 1998 (Cth).
[121] See s22 *Payment Systems (Regulation) Act* 1998 (Cth).

federal connections chosen to trigger the application of these sections were the involvement of "Commonwealth computers" in specifically prohibited incidents, or the commission of certain actions by means of "Commonwealth facilities" as defined within the section.

For the sections to apply, there must be some substantial connection with the Commonwealth or its interests, thus where the incident or its effects occur substantially within a particular state or territory, it is more likely that state or territorial provisions, if they exist and apply to the facts, will applied in preference to Commonwealth ones[122]. A similar preference is likely where Commonwealth facilities are the means by which computers physically located outside of Australia are wrongly interfered with, though the Act has extra jurisdictional effect[123].

The Wrongful Gaining of Access To Computers

The wrongful gaining of access to computers is prohibited and punished under sections 76B and 76D of the Act. The gaining of such access to "Commonwealth computers" is covered by s76B and may be committed in a *simpliciter* or three other aggravated forms. Section 76D is similarly drafted to cover mere access and aggravated forms to computers[124], but this is where the access has been effected by means of "a Commonwealth facility". The term "Commonwealth facility" is not defined in the Act, but it is clear from associated references to "a facility operated or provided by the Commonwealth or by a carrier"[125] that this includes telecommunications facilities. Unauthorised access to any computer, remotely achieved by means of services provided by any of the licensed telecommunications carriers or carriage service providers would thus fall, technically, within s76D, however it is unlikely to be so applied in practice unless a real and substantial Commonwealth link, or inter state complication is involved.

---

[122] State provisions are not pre-empted by the Commonwealth provisions - s76F *Crimes Act* 1914 (Cth), but the rule against double jeopardy in any event will preclude an offender being prosecuted more than once for the same offence. See for example s4C(2) *Crimes Act* 1914 (Cth) which provides that where an offender has been punished for an offend under the law of a State or Territory, that person shall not be liable to be punished for that same offence under the law of the Commonwealth, and s4K of the same Act which deals with continuing and multiple offences.

[123] See s3A *Crimes Act* 1914 (Cth).

[124] Whether designated as "Commonwealth" computers or otherwise.

[125] See ss76D(1) & 76E *Crimes Act* 1914 (Cth).

The *simpliciter* form of the offence requires no more than intentional and unauthorised access to the subject computer[126]. The *simpliciter* form of access is distinguished from access that is similarly intentional and unauthorised, but achieved in relation to specified categories of sensitive data[127]. Where the offender gains such access and knows or ought reasonably to know that it relates to such sensitive data, the episode will be regarded distinctly from the mere act of gaining access[128]. If the offender, having gained access to such data, continues to examine that data, the continued examination of the data will also constitute an offence[129].

The intentional gaining of unauthorised access with a fraudulent intention[130] is also covered by s76[131].

Altering Data or Impeding Access to Computers

Sections 76C and 76E of the Act make a wide variety of actions and effects on computers and the data contained therein unlawful. Prohibited effects upon data in computers, both Commonwealth related or otherwise[132] include the destruction of data, the erasure or alteration of data, or the insertion or addition of data[133]. It is also an offence to impede or prevent access to data, or to impair the usefulness or effectiveness of it[134], as it is to interfere with, interrupt, or obstruct the lawful use of a computer[135]. All such actions carry a maximum penalty of 10 years imprisonment.

---

[126] See s76B(1) & s76(D)(1). This carries a 6-month term of imprisonment. Access will still be regarded as unauthorised where a person with limited access rights exceeds such authority in accessing other parts or sections of a computer system.

[127] Data relating to Australian security, defence or international relations, law enforcement, the protection of public safety, the records of a financial institution, commercial information or trade secrets, or the personal affairs of any person - see ss76(B)(2)(b), 76(BD)(2)(b).

[128] See s76(B)(2)(b) & s76(D)(2)(b).

[129] See ss76B(3) and 76D *Crimes Act* 1914 (Cth).

[130] Specifically, the intent to defraud any person - see s76(B)(2)(a) and s76(D)(2)(a) *Crimes Act* 1914 (Cth).

[131] See s76(B)(2)(a) and s76(D)(2)(a) *Crimes Act* 1914 (Cth).

[132] Section 76C applies to Commonwealth computers, and computers in which data is stored on behalf of the Commonwealth, s76D to computers generally by means of Commonwealth facilities.

[133] See s76(C)(a), s76(C)(c) and s76(E)(a) *Crimes Act* 1914 (Cth).

[134] See s76(C)(d), s76(E)(c) *Crimes Act* 1914 (Cth)

[135] See s76(C)(b), s76(E)(b) *Crimes Act* 1914 (Cth).

A State Legislative Survey

Different approaches have been adopted in the various states with the result that differing aspects of computer related misconduct are criminalised to varying degrees in different states. The very different concepts and definitions adopted in each jurisdiction also mean that the national response is not generally speaking, uniform. This is unfortunate as the same action may be subject to different sanctions, if it is punishable at all, in individual states[136].

On a broad evaluation of state criminal statutes dealing with computer related offences three general approaches become apparent all of which are based on existing criminal statutes[137]. In many cases sui generis provisions have been inserted into existing statutes and located within or near sections dealing with property type offences. In other cases, the scope of existing provisions has been expanded by redefining traditionally understood concepts so that they specifically cover computer-related eventualities. In one case, existing criminal provisions were considered adequate, in the main, to meet envisaged computer related eventualities. It is also possible to identify other provisions relevant to limited aspects of computer misuse, that may provide a direct or indirect means for the prosecution of such misuse. However, these approaches have not been exclusively adopted - in roughly half of the states for instance, the first two approaches have been utilised in tandem[138].

Intercepting Telecommunications

An example would be the use of Internet filters to identify and copy credit card numbers sent unencrypted via the Internet to a remote location - such as in the context of a credit card purchase from an on-line mall. The *Telecommunications (Interception) Act* 1979 prohibits the interception of communications passing over a telecommunications system by prohibiting the listening to or

---

[136] The work of the Attorney-General's Model Criminal Code Officer's Committee on the development of a uniform Criminal Code for national application may go some way towards alleviating the uneven state coverage of computer related incidents.

[137] This may be contrasted for example with the British approach in which an independent statute, the *Computer Misuse Act* 1990 was enacted separately from the *Theft Act* 1968.

[138] See further, chapter five in Akindemowo, *Information Technology Law in Australia*, n87 at 215-222.

recording of communications in their passage over the telecommunications system, where this is done without the knowledge of the person making the communication[139]. The Act thus applies only to communications passing through systems for the transfer of electromagnetic energy, and the equipment that may be connected to it[140].

Unauthorised Telecommunications

The operation of an unlicensed telecommunications facility or the provision of telecommunication carriage services without license is an offence under the *Telecommunications Act* 1997[141]. Providers of telecommunications services and certain users of the telecommunications network are obliged to protect the confidentiality of information routed through the network by the Act[142]. Although constituted authorised recipients of such data, they may disclosure or use such data for those limited circumstances only that are specified as authorised under the Act[143]. Record-keeping obligations are also imposed[144].

It is thus an offence under the Act for such entities to use or disclose information or documents without authority or for an unauthorised purpose[145]. It is also an offence for any person to connect unlabelled[146], unauthorised, or dangerous equipment to the telecommunications network[147]. Where this has been done, and the network is damaged as a result, or the manager of the

---

[139] See s6(1) *Telecommunications (Interception) Act* 1979 (Cth).

[140] Radio communications for example are not covered by the Act. See P Grabosky & R Smith, *Crime in the Digital Age: Controlling Telecommunications and Cyberspace Illegalities*, Leichhardt NSW, The Federation Press, 1998 at 31.

[141] See for example s42 *Telecommunications Act* 1997 (Cth).

[142] For example, carriers, carriage service providers, number-database operators, emergency call persons and other eligible persons (including associates and contractors) - see ss271-275, and generally ss270-309 of the *Telecommunications Act* 1997 (Cth).

[143] An example purposes relating to the enforcement of the criminal law - see ss282 & 298 *Telecommunications Act* 1997 (Cth).

[144] See s270 and Part 13 of the 1997 Act generally.

[145] See ss276(3), 277(3), 278(3), 303 which cover the intentional or reckless disclosure of the contents or substance of a communication or the details of the personal affairs or particulars of a person connected with a communication. Sections 276-295 provide penalties of up to two years imprisonment for such offences. Both primary (ss279-295) and secondary (ss296-303) use/disclosures are covered.

[146] The connection of wrongly labeled equipment is also an offence - see s443-445 *Telecommunications Act* 1997 (Cth).

[147] See s448 of the *Telecommunications Act* 1997 (Cth).

telecommunications network concerned suffers loss or incurs liability as a consequence, the manager is provided with various remedial alternative by the Act: (a) the right to bring a civil action within three years of the damage or injury, (b) the right to seek in the alternative, damages or an account of profits for the wrongful connection, (c) the right to seek injunctive relief whether ex parte, interlocutory, or final, (d) the right to disconnect the offending equipment and any other equipment necessary to accomplish such disconnection[148].

MEETING THE LEGAL CHALLENGE

Arguments about what the legal response to the challenges of digitalisation should be have been fierce, and on occasion, misleading - such as where they have been inappropriately used to argue against the existence of the field of information technology law[149].

The legal response has in fact been varied. There have been many inquiries and reviews, amendments to existing laws, and new laws both technology neutral and technology dependent enacted. Voluntary codes have been developed and adopted and informal supervisory regimes been implemented.

Controlling Abuses: The Regulation Debate

The varied legal response is further reflected in the rather narrower concern about whether the Internet can and should be regulated. The jury is still out on this, but the signs are that most jurisdictions are leaning in the direction of (attempts at) regulation, though jurisdictions such as Australia are inclined to trial rather less intrusive forms as a first step.

The risks arising from the widespread use of the Internet provide one argument in favour of its regulation - the potential magnitude of

---

[148] See ss443-449 *Telecommunications Act* 1997 (Cth). Disconnection may be sought where the equipment is unlabelled, dangerous, or otherwise poses a threat to the integrity of the network - ss445-447 of the 1997 Act. Where the ACA determines however, that there were no reasonable grounds for such disconnection, the manager may be found liable in an action brought by persons suffering loss or damage as a result of the disconnection of the equipment, (if brought within three years) and ordered to provide relief, and/or the manager may be ordered to reconnect the equipment.

[149] For example, by misconstruing arguments and using as a premise alleged calls for sui generis legislation. See above.

financial frauds, money laundering, tax evasion, and other unlawful acts has tended to stimulate calls for regulation from financial system and taxation regulators in certain countries. The immense power base that the Internet may constitute, through the knowledgeable exploitation for evil or good by any number of persons, is a further matter of concern for law enforcement agents[150]. The prescriptive and remedial functions of the law may also be called in aid of arguments in favour of more formal regulation.

The arguments however are not one-sided and they continue to be vigorously debated. The historical antecedents of the Internet are often mentioned in this regard to support the point that the Internet would probably not exist in its present form, if it would have come into being at all, if the voluntary networking and technologically creative excursions upon which its inception was based, had been regulated. It is also argued that the development of the medium, still being in an early phase, would be artificially diverted or is potential stifled by regulation. The etiquette of the Internet[151] is also mentioned as a relatively effective means of regulating Internet behaviour, and in any case, it is argued, there is nothing wrong with the functioning of the Internet. It is often argued in this regard that the risks of Internet use can be managed by means other than those involving formal regulation, and in any case, "if it ain't broke, don't fix it". Others while admitting that the risks are indeed a cause for concern, have taken the view that it would be a vain task to attempt to regulate the Internet, as this is not practically possible.

Although this last argument is certainly debatable, it is the case that certain factors presently prevailing, would operate to hinder the effective regulation of the Internet if attempted. Technological concerns, for instance the difficulties involved in monitoring or tracing the immense volumes of data that would be involved are one example. Practical factors such as legislative concerns[152], the need for international cooperation[153], the involvement of lobby groups or

---

[150] The Internet is in fact already being used for a number of unlawful purposes such as tax evasion, money laundering, the promulgation of pornographic or other offensive material, the inciting of racial hatred, and of course, consumer fraud.

[151] Often referred to as "netiquette", this may include the blackballing and ignoring or blocking out of persons engaging in offensive behaviour.

[152] Such as the time and effort involved in the successful passage of legislation, and the risks of legislative obsolescence, redundancy or ineffectiveness due to the intensely dynamic nature of the subject matter.

[153] And possible associated difficulties such as the holding of different official policies, disparities in the strengths and strategies of lobby group equivalents in different

interest groups[154], and the anarchical tendencies in this regard of a not insignificant proportion of Internet users are others. Concerning the latter factor, the prospect of repressive regulation or indeed any formal regulation at all, has roused a variety of responses ranging from the liberal to the fiercely individualist to the militantly anarchical[155]. The anti-regulation stance adopted by some serving as a rallying cry for wide groups of interests determined to ensure that the Internet remains a free frontier, the response has encompassed the pooling of expertise, and in more radical circles, recommendations and the implementation of subversive tactics, to subvert any implementation of formal regulatory policy.

Although the outcome of this continuing debate remains uncertain, an increasing number of formal inquiries and provisional policy statements, particularly at the international level, appear to be more in favour of regulation than against. In such cases the objectives given priority in order of decreasing importance, tend to be the minimising of harm, the protection of rights of expression, privacy or association, and the avoidance of any hindering of the relevant technology's development.

Policy decisions may also be made as to the degree of objectionableness of certain actions or types of content - actions or content which is intrinsically harmful, content to which access ought to be restricted[156], content which individuals ought to be able to avoid if desired, and unobjectionable content that ought to be freely available, although the division of content into such categories may not be a straightforward task. The form of regulation, if any, that may be considered desirable to apply to such situations may range from total prohibitions backed by criminal sanctions, to the application of

---

countries, bureaucratic delays, and of course, the inevitable time lags associated with such efforts.

[154] The history of the several attempts to pass state privacy legislation is a good illustration of the influence or impotence (depending on the lobby under consideration) of certain lobby groups upon the enactment of legislation in Australia - see for example, chapter six of O. Akindemowo, *Information Technology Law in Australia*, (LBC Information Services, Sydney, 1999).

[155] Illustrative of the intense hostility suggestions for the regulation of the Internet has roused in some quarters was the response to the US Decency in Communications Act 1997 which was declared unconstitutional in *ACLU v. Reno* 929 F Supp 824; 117 S Ct (ED Pa 1996) 2329 (1997). Another example was the apparently widespread adoption of the Internet Blue Ribbon Campaign mounted by Electronic Frontiers Australia in 1995.

[156] See for example the *Broadcasting Services Amendment (Online Services) Bill* 1999. Technological aids such as content filters may play a part in the enforcement of such policies.

administrative regulations, to the use of codes of conduct[157], to the provision of a choice of voluntary options.

In the interim, compromise measures are being taken. These include the application of selective rather than wide ranging controls[158], the establishment of international cooperative initiatives for the sharing of data by law enforcement agencies, and recommendations within specifically limited contexts, for the passage of local level provisions of extra territorial application[159].

Concluding in Context

The complexity of matters arising from the pervasive influence of the Internet, and digital technology is such that issues ought not, and indeed can not any longer, be considered in a vacuum, or in the abstract, profitably. Any consideration of the issues that have arisen, and are likely to arise in the future must be evaluated from a wide perspective, informed by related matters or legal principles. This is one of the strengths of information technology law, in that it provides a context for an informed consideration of matters, lessening the risk of misinformed, or inexpert analyses of the legal complexities arising from the use of information technology.

---

[157] Suggestions advocating co-regulation, a combination of formal regulation and self-regulation measures, are becoming common and more popular. A number of Codes of Practice for the regulation of the Internet Industry are currently under development - see for example the work of Internet Industry Association (IIA) available from http://www.iia.net.au/index3.html

[158] Examples of this are the suggestions that have been made for the regulation of issuers of digital cash rather than all participants in electronic cash systems, or the imposition of restrictions on select features rather than all features of specified facilities.

[159] And on the national level, the amendment of local laws to facilitate the prosecution of some forms of Internet illegality. See for example the Electronic Commerce Expert Group's Deliberations - Issues Paper No.1 and Final Report available at http://law.gov.au/aghome/advisory/ (last visited November 1998).