Electronic Contract Administration – Legal and Security Issues Literature Review

Report No. 2005-025-A

The research described in this report was carried out by: Ed Dawson, Sharon Christensen, Ernest Foo, Audun Josang, Praveen Gauravaram, Kathryn O'Shea and Judith McNamara.

Project Leader	Sharon Christensen (QUT LAW)
Team Members	Sharon Christensen, Bill Duncan (QUT LAW) Ed Dawson, Ernest Foo, Audun Josang (QUT IT/Security) Martin Betts, Debbie Smit (QUT BEE) Kerry London (UN)
Researchers	Kathryn O'Shea (QUT LAW) Judith McNamara (QUT LAW) Praveen Gauravaram (QUT IT/Security)
Project Affiliates	Ross Guppy (QDMR) Michael Austin, Dayv Carter (QDPW) Neil Abel (BCC) Gerry Shutt, Geoff Gannon (JHG)

Research Program No:	A
Program Name:	Business and Industry Development
Research Project No.:	2005-025-A
Project Name:	Electronic Contract Administration – Legal and Security Issues
Date:	13 June 2006

Distribution List

Cooperative Research Centre for Construction Innovation
Sharon Christensen, Bill Duncan, Kathryn O'Shea, Judith McNamara (QUT LAW)
Ed Dawson, Ernest Foo, Audun Josang, Praveen Gauravaram (QUT IT/Security)
Martin Betts, Debbie Smit (QUT BEE)
Kerry London (UN)
Ross Guppy (QDMR)
Michael Austin, Dayv Carter (QDPW)
Neil Abel (BCC)
Gerry Shutt, Geoff Gannon (JHG)

Disclaimer

The Client makes use of this Report or any information provided by the Cooperative Research Centre for Construction Innovation in relation to the Consultancy Services at its own risk. Construction Innovation will not be responsible for the results of any actions taken by the Client or third parties on the basis of the information in this Report or other information provided by Construction Innovation nor for any errors or omissions that may be contained in this Report. Construction Innovation expressly disclaims any liability or responsibility to any person in respect of any thing done or omitted to be done by any person in reliance on this Report or any information provided.

Please direct all enquiries to:

Chief Executive Officer
Cooperative Research Centre for Construction Innovation
9th Floor, L Block, QUT, 2 George St
Brisbane Qld 4000
AUSTRALIA
T: 61 7 3864 1393
F: 61 7 3864 9151
E: enquiries@construction-innovation.info
W: www.construction-innovation.info

Table of Contents

PREFACE

The Cooperative Research Centre (CRC) for Construction Innovation research project 2005-025-A *Electronic Contract Administration – Legal and Security Issues*, is supported by a number of Australian industry, government and university based project partners, including: Queensland University of Technology, Queensland Department of Public Works, Queensland Department of Main Roads, Brisbane City Council, University of Newcastle and John Holland Pty Ltd.

In support of this project's research aims and objectives, and as a deliverable for the project, this Report contains the results of a literature review of various national and international publications relating to electronic contracting. The Report is intended to identify the legal and security issues that may arise where Australian building and construction contracts are formed, administered and recorded within an electronic environment.

EXECUTIVE SUMMARY

A review of the relevant literature, legislation and judicial decisions of the courts reveals that the following legal and security issues may arise in connection with the electronic formation, administration and recording of Australian construction contracts (and associated documents):

Electronic Contract Formation (Section 3 of this Report)

- There are legal uncertainties when determining the precise point in time that an electronic construction contract has been formed.

- There are legal uncertainties when determining *where* an electronic construction contract has been formed.

- If a construction contract contains a guarantee, there are statutory provisions that render the guarantee unenforceable if the guarantee (or some memorandum or note of it) is not in writing and signed by the party to be charged. There are legal uncertainties about whether an electronic communication will satisfy these statutory writing and signature requirements.

- If an offer to enter into a construction contract specifically requires acceptance to be communicated in writing, there are doubts about whether an electronic communication of acceptance will be effective to form an enforceable contract.

Electronic Contract Administration and Management (Section 4 of this Report)

- The exchange of electronic communications between parties may, depending upon the terms and conditions of a construction contract, amount to an effective variation of the contract.

- Depending upon the terms and conditions of a construction contract, there may be legal uncertainties about the validity of electronic notices.

- Protocols need to be established to ensure that electronic documents viewed by all project participants are identical. It is important that each project participant is using the same software and settings to ensure that all participants view the same document.

- Online collaboration platforms are emerging as the principal tool used in electronic contract administration and management in the construction industry. A range of legal issues may be encountered in relation to the use of collaboration platforms.

Electronic Records Management (Section 5 of this Report)

- The effective management of construction projects necessarily entails a range of communications passing between a large number of project participants. Where these communications occur electronically, a number of complex legal issues arise about whether or not the electronic communications may be used as evidence and the evidential weight that may be attributed to them.

- There is legal uncertainty as to whether electronic records relevant to a construction project can be relied upon as evidence in court.

- It is uncertain whether electronic records will be given the same weight in court as their paper based equivalents.

- Electronic records must be carefully managed to ensure that construction project participants are in a position to comply with their discovery obligations in the event of litigation.

- Construction project participants must preserve electronic records in a way that satisfies all legal requirements governing the retention of records.

1. INTRODUCTION

1.1 Background

The Co-operative Research Centre (CRC) for Construction Innovation research project 2002-067-A *E-business – Security and Legal Issues* (the 'E-tendering Project') identified a range of legal and security issues that may be encountered in electronic tendering in the construction industry. In addition to the myriad of issues that were identified in connection with electronic tendering, the E-tendering Project revealed that if industry participants wished to proceed to the next stage of development, being the formation of contracts in a wholly electronic environment, further research in both the legal and computer security fields would be warranted.

This Report is a deliverable for the CRC for Construction Innovation research project 2005-025-A *Electronic Contract Administration – Legal and Security Issues*. It contains the results of a literature review of various national and international publications, legislation and court decisions relevant to electronic contracting. The Report identifies the legal and security issues that may arise in connection with:

- The formation of construction contracts within an electronic environment;
- The electronic administration and management of construction contracts; and
- The management and retention of electronic records associated with construction projects.

1.2 Report structure

This Report is structured as follows:

- Section 2 contains an overview of some of the recent activities of international organisations in the areas of electronic contracting and commerce.
- Section 3 considers the legal and security issues that may arise in the formation of construction contracts in an electronic environment.
- Section 4 examines the legal and security issues that may arise in the electronic administration and management of construction contracts.
- Section 5 provides an overview of the legal and security issues that may be encountered in the management and retention of electronic records associated with construction projects.
- Section 6 is a general summary of the legal and security issues that have been identified in this Report.

2. OVERVIEW OF ACTIVITIES BY INTERNATIONAL ORGANISATIONS

2.1 Introduction

The increasing use of information and communication technology (ICT) as an effective business tool has prompted a number of international organisations to investigate the legal consequences that may flow from using ICT as a medium to form contractual relationships.

Section 2.2 provides a brief overview of some of the recent and relevant activities of a number of international organisations performing work in the areas of electronic commerce and contracting. The overview of international activity is not intended to be exhaustive and relates particularly to international Directives, Conventions or Model Laws that may have an impact upon the laws in Australia.

2.2 Overview of activities by various international organisations

- **United Nations General Assembly** – On 23 November 2005 the United Nations General Assembly resolved to adopt a new Convention on the Use of Electronic Communications in International Contracts. The Convention seeks to ensure that electronically negotiated contracts are as valid as traditional paper based contracts, and to enhance legal certainty and commercial predictability where electronic communications are used in international transactions (United Nations 2005). The terms of the Convention are similar, but not identical to the existing electronic transactions legislation that has been enacted in Australia.

  The new Convention builds upon previous Model Laws prepared by UNCITRAL (as discussed below) and is the first attempt by the United Nations to address electronic transactions in a way that binds Member States when they ratify the Convention by passing domestic laws to give effect to it (Connolly & Ravindra 2005). The Convention is available for signature by Member States from 18 January 2006 until 16 January 2008. As at the date of this Report, Australia has not signed the Convention.

- **United Nations Commission on International Trade Law (UNCITRAL)** – UNCITRAL's general mandate is to progress the unification and harmonisation of the laws that govern international trade. It has a number of working groups, including Working Group IV on electronic commerce. UNCITRAL has been responsible for a number of developments in the area of electronic transactions, including the preparation of the following Model Laws and recommendations:
  - UNCITRAL Model Law on Electronic Signatures 2001 – Australia has not passed legislation to implement the recommendations of this Model Law.
  - UNCITRAL Model Law on Electronic Commerce 1996 – This Model Law was designed to give national legislators a set of internationally acceptable rules to promote the use of electronic communications. Australia has enacted uniform domestic legislation based on the Model Law, in the form of the *Electronic Transactions Act 1999* (Cth) and mirror State legislation.
  - UNCITRAL Recommendation on the Legal Value of Computer Records 1985.

- **United Nations Economic Commission for Europe (UNECE)** – The UNECE has developed the United Nations Centre for Trade Facilitation and Electronic Business (UN/CEFACT), with the principal focus of facilitating national and international transactions through the harmonisation and simplification of procedures and processes. Among other things, UN/CEFACT has published a range of Trade Facilitation Recommendations, including a recommended electronic commerce agreement. The underlying purpose of the recommended agreement is to enable business to business electronic commercial transactions to be conducted in a manner that is legally sound (UNECE 2000).

- **United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP)** – UNESCAP has performed various investigations into the harmonisation of e-commerce laws in the Asia and Pacific regions. In July 2004, it convened a Regional Expert Conference on the 'Harmonized Development of Legal and Regulatory Systems for Electronic Commerce in Asia and the Pacific – Current Challenges and Needs'. One outcome of the conference has been the production of an information note outlining the general legal issues that may be encountered in electronic transactions (UNESCAP 2005).

- **European Commission (EC)** – The European Parliament and the Council of the European Union have passed several directives that impact upon the process of e-contracting in the European Union, including: Directive 1999/93/EC of 13 December 1999 on a community framework for electronic signatures ('Directive on Electronic Signatures') and Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on Electronic Commerce'). In essence, EU Member States are bound to follow the objectives of the Directive on Electronic Signatures and the Directive on Electronic Commerce, but have the discretion to decide how and in what form the objectives are achieved when passing national legislation to give effect to them.

- **International Chamber of Commerce (ICC)** – The ICC has a number of different task forces, including task forces on jurisdiction and applicable law in electronic commerce, and electronic contracting. The ICC has produced a number of publications in the area of electronic transactions, including the ICC eTerms 2004 (which are very basic terms designed to increase the legal certainty of electronic contracts) (ICC 2004), and GUIDEC II – General Usage for Internationally Digitally Ensured Commerce, a document intended to educate business on various techniques in electronic commerce, and to set a general framework for the authentication of digital messages (ICC 2001).

- **Organisation for Economic Co-operation and Development (OECD)** – The OECD has a Working Party on Information Security and Privacy that has investigated a range of issues relating to authentication and electronic signatures. Among other things, in 2005 the OECD published a report on the use of authentication across borders in OECD countries, examining the actual or potential barriers to the cross-border use of digital signatures as identified from survey responses provided by both government and the private sector in a number of OECD countries (OECD 2005).

- **Commonwealth Secretariat** – The Law Development Section of the Commonwealth Secretariat has produced several Model Laws that deal with issues relevant to electronic transactions. More specifically, it has produced the following draft Model Laws:
  - Draft Model Law on Electronic Transactions – This Model Law is designed largely to assist common law countries when domestically implementing UNCITRAL's Model Law on Electronic Commerce 1996.
  - Draft Model Law on Electronic Evidence - This Model Law is intended to assist common law countries to develop appropriate legislation that caters for electronic evidence.

2.3 Global legislative activity

In addition to the research conducted by international organisations, there has been 'an explosion of legislative activity around the world in attempts to regulate and guide the development of e-commerce' (Lawrence 2000, p85). UNCITRAL's Model Law on Electronic Commerce 1996 has now been enacted in (or influenced the development of) domestic legislation in a large number of countries including, for example, the United States, the

United Kingdom, Australia, New Zealand, Canada, Singapore, China and Korea. Although the legislation in these countries is not identical, the key issues that have been targeted for resolution in most jurisdictions are the legality and enforceability of electronic contracts (Lawrence 2000, p85).

In an Australian context, the ability of our legal system to ensure the legality and enforceability of electronic contracts will depend upon whether our general law principles, electronic transactions legislation and rules of evidence adequately address the unique legal issues that may arise from using modern communication technologies to form, administer and record electronic contracts. Sections 3, 4 and 5 of this Report consider these issues.

3. ELECTRONIC CONTRACT FORMATION

3.1 Overview of issues associated with electronic contract formation

A review of the relevant literature, legislation and decisions of the courts reveals that the following legal issues may arise when forming building and construction contracts in an electronic environment:

- There are legal uncertainties when determining the precise point in time that an electronic construction contract has been formed. (Refer to section 3.6)

- There are legal uncertainties when determining *where* an electronic construction contract has been formed. (Refer to section 3.7)

- If a construction contract contains a guarantee, there are statutory provisions that render the guarantee unenforceable if the guarantee (or some memorandum or note of it) is not in writing and signed by the party to be charged. There are legal uncertainties about whether an electronic communication will satisfy these statutory writing and signature requirements. (Refer to section 3.10 for writing requirements, and section 3.12 for signature requirements)

- If an offer to enter into a construction contract specifically requires acceptance to be communicated in writing, there are doubts about whether an electronic communication of acceptance will be effective to form an enforceable contract. (Refer to section 3.11)

Each of these issues is expanded upon in the sections below. It should also be noted that a number of other legal issues are discussed in section 3 of this Report, which have not been included in this overview summary. These issues have been omitted from the summary because the legal principles that resolve them will remain the same, regardless of whether or not a construction contract is formed in a paper based or electronic environment.

3.2 General legal principles governing the formation of all contracts

On a fundamental level, a contract may be considered to be an agreement between parties that a court will enforce. An electronic contract or ‘e-contract’ may simply be described as a contract that has been formed through the use of electronic communications.

Under the general law, the following five basic elements must be present before a court will enforce a contract (Willmott, Christensen & Butler 2005):

- An offer.
- Acceptance of the offer.
- Certainty – from an objective viewpoint, a court must be able to ascertain exactly what the parties have agreed. An often quoted statement of this rule is that:

> In order to constitute a valid contract the parties must so express themselves that their meaning can be determined with a reasonable degree of certainty. (*G Scammell and Nephew Ltd v HC and JG Ouston* [1941] AC 251 at 255).

- Intention – from an objective viewpoint, the parties must intend that their agreement will be legally binding.
- Consideration – for a contract to be enforceable, it must be supported by consideration. Consideration may be generally defined as the price that is paid in return for a promise.

> To enforce a promise made by one party, the other party must do (or agree not to do) something in return for the promise.

These basic principles of contract law have been developed over the years through the judicial decisions of the courts. The current judicial trends indicate that these principles will apply to all contracts regardless of whether they are formed electronically, orally or through paper based communications. Many of the issues that arise for consideration relate to how these traditional contract law principles will apply to modern forms of technology.

3.3 Additional legal principles consequent upon a shift to an electronic environment

In addition to traditional contract law principles, each jurisdiction in Australia has passed uniform electronic transactions legislation based upon UNCITRAL's Model Law on Electronic Commerce 1996 (aimed at addressing some of the legal uncertainties that have arisen from the increasing use of electronic communications to conduct transactions). In Queensland, the relevant legislation is known as the *Electronic Transactions (Queensland) Act 2001* (Qld) ('ETQA'). As electronic contracts are governed by both general contractual principles and the ETQA, it is important to consider both of these sources when determining the legal issues that may arise in electronic contracting.

It has been noted by various commentators that the ETQA (and associated electronic transactions legislation around the country) adopts a 'minimalist' or 'light handed' regulatory approach. It is not designed to provide a comprehensive legal framework offering certainty for all legal aspects of electronic transactions, nor does it mandate the use of a particular form of technology (De Zilva 2003, p1010; Lawrence 2000, p89). The object of the ETQA (as set out in the Act) is to provide a regulatory framework that:

(a) recognises the importance of the information economy to future economic and social prosperity;

(b) facilitates the use of electronic transactions;

(c) promotes business and community confidence in the use of electronic transactions; and

(d) enables business and the community to use electronic communications in their dealings with government.

To give effect to these objectives, the ETQA relies on two fundamental principles: functional equivalence (meaning that equal treatment should be given to both paper based and electronic transactions); and technology neutrality (meaning that the law will not discriminate between different forms of technology).

These general principles are embodied by s 8 of the ETQA, which establishes that transactions are not invalid under a State law merely because they take place wholly or partly by one or more electronic communications. The way the ETQA defines a 'transaction' clearly includes contracts and agreements. However, this general rule can be displaced by more specific provisions that are contained in Chapter 2 of the ETQA.

Accordingly, when considering the application of the ETQA, regard must be had to specific provisions of the Act which may, subject to certain conditions being established, allow the following matters to be met electronically:

- a requirement to give information in writing (s 11 ETQA);
- a permission to give information in writing (s 12 ETQA);

- a requirement for a signature (s 14 ETQA);
- a requirement to produce a document (s 16 ETQA);
- a permission to produce a document (s 17 ETQA);
- a requirement to record information in writing (s 19 ETQA); and
- a requirement to keep a written document or electronic communication (ss 20 and 21 ETQA).

The interplay of the ETQA and general law contractual principles may give rise to various legal issues and uncertainties for electronic contracting. These issues are considered below, following a general discussion about the various technical ways that electronic contracts may be formed.

3.4 Methods of electronic contracting

Electronic contracts may be formed in a number of different ways. Some examples of the different methods that may be used to form electronic contracts include:

- **Contract formation through electronic communications:** The simplest electronic contract is formed by the exchange of text documents via electronic communications such as email.

- **XML-Contracts:** The text documents that form the basis of an electronic contract may be written in XML. XML is an abbreviation for extensible markup language. It is a markup language for documents containing structured information (Walsh 1998). Structured information contains both content and some indication of what role that content plays. One advantage of forming contracts using XML is that contracts can be processed using machines and contracts can be imported into contract management and negotiation tools. A further advantage to using XML is achieving better specifications of the contract using industry specific XML vocabularies.

- **‘Click to agree’ contracts:** An electronic contract may be in the form of a ‘click to agree’ contract. The terms and conditions of the contract are displayed on one party’s website and the other party (e.g. the customer) agrees to the contract by clicking an ‘I agree’ button on the website accepting the relevant terms and conditions. This type of electronic contract is commonly used for the purchase of downloaded software. Once the transaction is completed, the issuer of the contract ordinarily sends an email to the customer (which may be automatically generated) confirming the details of the transaction.

Generally, when parties decide upon a particular method of electronic contract formation, their decision is influenced by the nature and importance of the relevant contract. For contracts of strategic importance or of high economic value, parties may wish to utilise appropriate technology that ensures the security and authenticity of relevant documentation.

3.5 General legal recognition of electronic contracts

Although complicated legal issues may arise in the formation of contracts by electronic means, there is no overriding legal impediment to parties using electronic communications to form contractual relationships.

As a general principle, the law does not require a binding contract to be established by any particular communication method. Accordingly, most contracts may be formed by any number of methods including, for example, by the post, telex, facsimile or even orally. The important principles remain the same regardless of the technology that is used to create the contract - in other words, to create a binding contract the five legal elements outlined in section 3.2 above must be present.

An example of where the courts have upheld a contract formed by electronic means is the decision in *Ford v La Forrest* [2001] QSC 261, where it was found that emails are capable of creating a binding contractual relationship. Whilst the ETQA does not provide an impenetrable rule that all electronic transactions will be valid in all circumstances, the general position that contracts may be formed by electronic communications is strengthened by s 8 of the ETQA. Section 8 of the ETQA sets out the general rule that transactions (including contracts) are not to be rendered invalid under a State law simply because they take place wholly or partly by one or more electronic communications.

While parties are free to use electronic communications to form most contracts, the discussions below highlight that the use of electronic communications may present a number of legal hurdles or uncertainties in the contract formation process.

3.6 Determining the point in time that an electronic construction contract is formed

3.6.1 General law contractual principles

One of the main reasons why it may be important to determine the precise point in time that an electronic construction contract has been formed, is that once an offer has been accepted it becomes irrevocable (*Great Northern Railway Co v Witham* (1873) LR 9 CP 16). Accordingly, up until the point in time that the offer has been accepted (being the time that the contract is formed) the offeror is free to withdraw the offer. The time of contract formation will also impact upon an analysis of where the contract has been formed (refer to section 3.7 below).

Under general law contractual principles, it is an established rule that the acceptance of an offer (which constitutes the formation of a contract) is effective at the time it is communicated to the offeror (*Byrne & Co v Leon Van Teinhoven and Co* (1880) 5 CPD 344). When communication takes place, it is said that at this point in time there is a ‘meeting of the minds’ of the parties as they have reached agreement or consensus upon the terms of the contract (Hill 2002, p4). However, there is an exception to this general rule known as the ‘postal acceptance rule’.

The postal acceptance rule generally applies where the post is used as the method of communication between the parties. If the rule applies, then the general position is changed such that the acceptance of an offer becomes effective (and the contract is formed) at the time the acceptance is *posted*, rather than at the time the acceptance is *communicated* to the offeror (*Henthorn v Fraser* [1892] 2 Ch 27).

The question to be resolved is whether or not the postal acceptance rule will apply to emails and other forms of electronic communications (for example, messages that are communicated online through a website collaboration platform).

Application of the postal acceptance rule to electronic communications

There has been no definitive judicial statement about whether or not the postal acceptance rule will apply to email or various other relatively recent communication technologies. It has, however, been established that the rule will not apply to communications by telephone, telex and facsimile.

The only judicial consideration of this issue in connection with modern communication technologies, appears in the first instance judgment of the Singapore High Court in *Chwee Kin Keong v Digilandmall.com Pte Ltd* [2004] 2 SLR 594. The comments made in the case were not necessary to decide the issue before the court, so the judge did *not* give any definitive views about how this important issue should be determined. However, the various statements made by the judge in this case appear to suggest that in the case of emails, it may be inappropriate for the postal acceptance rule to apply. For transactions that are conducted over the world wide web, it was suggested that as these transactions are ‘almost invariably instantaneous and/or interactive’, the logical default rule should be the usual position that acceptance will be effective when it is received (at [101]).

The application of the postal acceptance rule to email has been the subject of debate by numerous commentators. The following arguments have been raised on this issue:

- It is likely that the courts will categorise email as a virtually instantaneous form of communication. Accordingly, the postal acceptance rule should not apply and acceptance should be effective upon communication (O’Shea & Skeahan 1997, p259; Hill 2001, p51; Hill 2002, p6; Nikolich 2003, p28; Department of Justice Canada 2005, p9-8).

- Classifying email as an instantaneous or non-instantaneous form of communication may be inappropriate. Taking into account a variety of factors (such as the technology being used, business practice, the intention of the contracting parties and legislation designed to facilitate electronic commerce) the general principle that acceptance is effective upon communication should be applied in the first instance. Only if the parties have provided otherwise should a different time of acceptance be adopted (Christensen 2001, p38).

- Email is not instantaneous - email messages may be delayed or even lost as a consequence of a variety of occurrences (for example system crashes, network congestion or power outages) and it may be the case that a sender never knows whether a message has been received. Accordingly, it may be argued that email acceptances should receive the benefit of the postal acceptance rule (Lim 2002, pp 65-6). Other commentators have used the fact that emails may be lost or corrupted to argue that it would be unreasonable to apply the postal acceptance rule to email communications (Argy & Martin 2001, p21).

- As communications by email are similar to posting a letter, the postal acceptance rule should apply to an acceptance sent by email. Accordingly, acceptance should be effective at the time that an offeree sends the acceptance email (Pitiyasak 2003, p21). In contrast where electronic contracts are formed through websites, the parties communicate instantaneously therefore the postal acceptance rule should not apply (Pitiyasak 2003, p20).

- Whether the postal acceptance rule applies may be influenced by the functionality of the technology used to communicate the acceptance of an offer, as this may influence an assessment of which party should ultimately bear the risk of non-receipt of the acceptance communication (Hogan-Doran 2003, p378). Accordingly, differences in technology may mean that the postal acceptance rule will continue to be relevant for some forms of technology.

As can be seen from the above arguments, the applicability of the postal acceptance rule to electronic communications is uncertain. This is particularly the case as there is a broad range of communication technologies that may be used in electronic contracting, such that it may be argued that no ‘one rule fits all’. Accordingly, this issue will only be resolved by a definitive judicial statement by the courts or by legislative intervention.

Even if it can be assumed that the postal acceptance rule does not apply to electronic communications and that acceptance is effective when communicated to an offeror, there is a debate about when ‘communication’ actually occurs. For example, if the acceptance is sent by email, the various options for when the email is communicated could include: the time when the recipient reads the message; the time that the message is downloaded to the recipient’s computer; or the time when the message is received by the recipient’s ISP (Christensen 2001, p33).

Accordingly, a number of uncertainties exist when determining the point in time that an electronic construction contract will be formed under general law contractual principles. Unfortunately, as discussed below, these uncertainties have not been clarified by the ETQA.

3.6.2 *Electronic Transactions (Queensland) Act 2001* (Qld)

Sections 23 and 24 of the ETQA attempt to clarify when an electronic communication is dispatched and when it is received. These provisions are reproduced below:

> **23 Time of dispatch**
>
> (1) If an electronic communication enters a single information system outside the control of the originator of the communication, then, unless otherwise agreed between the originator and the addressee of the communication, the dispatch of the communication occurs when it enters the information system.
>
> (2) If an electronic communication enters successively 2 or more information systems outside the control of the originator of the communication, then, unless otherwise agreed between the originator and the addressee of the communication, the dispatch of the communication occurs when it enters the first of the information systems.
>
> **24 Time of receipt**
>
> (1) If the addressee of an electronic communication has designated an information system to receive electronic communications, then, unless otherwise agreed between the originator of the communication and the addressee, the time of receipt of the communication is the time when it enters the information system.
>
> (2) If the addressee of an electronic communication has not designated an information system to receive electronic communications, then, unless otherwise agreed between the originator of the communication and the addressee, the time of receipt of the communication is the time when it comes to the attention of the addressee.

One of the main problems with the ETQA provisions is that while they do state when an electronic communication is dispatched and when it is received, they *do not*, in a contractual framework, state whether it is the sending or the receipt of the electronic communication that completes the formation of a contract (Hill 2001, p46; Thomson 2003, p27; De Zilva 2003, p1020). The ETQA provisions could therefore be viewed by a court as either supporting the usual rule that acceptance is effective upon communication, or be seen to leave the question of when an acceptance is effective to general law contractual principles (Christensen 2001, p38).

Accordingly, the ETQA does not answer the question of whether or not the postal acceptance rule will apply to electronic communications. Even if it could be assumed that acceptance of an offer is effective upon communication, s 24 of the ETQA (which specifies the time of receipt of electronic communications), does not definitively settle all relevant timing issues. A review of the literature reveals the following further issues under the ETQA:

- Under the ETQA, the effective time of receipt of an electronic communication depends upon whether or not the addressee has *designated* an information system to receive electronic communications. However, when can an addressee be said to have *designated* an information system? For example, for designation to occur, does an offer have to specifically state an email address to which the acceptance should be sent, or will the automatic inclusion of a return email address in an email message be enough for designation to occur? (Giles 2000, p12).

- If the addressee has designated an information system, then receipt of an electronic communication is generally effective when the communication enters the information system. The ETQA definition of an 'information system' is extremely broad and depending upon the relevant context, may mean any number of things.

- If the addressee has not designated an information system, then generally speaking the time of receipt is 'when it comes to the attention of the addressee'. Questions arise as to when this occurs – for example, is it necessary that the addressee actually read the communication? Clause 14 of the Revised Explanatory Memorandum to the *Electronic Transactions Bill 1999* (Cth) suggests this is not necessary. It provides that:

  > The term "comes to the attention of the addressee" does not mean that a communication must be read by the addressee before it is considered to be received. An addressee who actually knows, or should reasonably know in the circumstances, of the existence of the communication should be considered to have received the communication. For example, an addressee who is aware that the communication is in their electronic mail 'box' but who refuses to read it should be considered to have received the communication.

  It has been suggested that even this clarificatory statement is still not sufficient to resolve the question of when an electronic communication may be said to 'come to the attention of the addressee' (Thomson 2003, p27). However, the statement does appear to reflect some of the rules that have developed under the general law which recognise that on occasion, it may be necessary to deem a person to have received a communication (Hill 2002, p8).

Accordingly, under both the general law and the ETQA, legal uncertainties exist about determining the precise point in time that a contract will be formed by electronic communications. It has been suggested that the safest way to avoid these complications and to achieve certainty, is to include clear provisions in the contractual offer which specify how acceptance is to be communicated and when an acceptance of the offer will be considered effective (O'Shea & Skeahan 1997, p262; Hill 2002, p10). Appropriately drafted provisions would be effective to avoid the uncertainties under the general law and the ETQA about the time that a contract is formed.

In addition to ensuring that appropriate timing provisions are included in a contract, from an evidentiary perspective it will be important to ensure that the date and time of electronic communications are accurately recorded. The technical methods that may be adopted for secure time recording are discussed in section 5.3.4 below.

3.6.3 Conclusion

Under both the general law and the ETQA, there are legal uncertainties which make it difficult to ascertain the precise point in time that an electronic construction contract will be formed. These uncertainties may be avoided by including clear provisions in a contractual offer which specify how acceptance is to be communicated, and when an acceptance of the offer will be deemed to be effective.

3.7 Determining where an electronic contract has been formed – jurisdictional issues

As can be seen from the discussions in section 3.6 above, difficulties may be encountered when determining the exact point in time that an electronic construction contract has been formed. In essence, it is uncertain whether acceptance of an offer takes place at the time the acceptance is sent by the offeree, or at the time that it is communicated to the offeror. These uncertainties also mean that it is difficult to determine *where* the contract is formed.

The reason why it may be important to ascertain *where* a particular contract has been formed, is that the place of contract formation may provide a court with jurisdiction to hear and determine a dispute under the contract. A court may assume jurisdiction over a contractual dispute in a number of circumstances, including where the contract is: made within the jurisdiction; governed by the law of the forum; or broken within the jurisdiction (Hill 2001, p49). Hill (2001, p49) provides the following simple example that illustrates how problems in determining the time that a contract is formed, translate into problems in establishing *where* the contract has been formed:

> As an example, take a sale of goods where the contract is formed via email. If we take it as given that the *offer* is made by the buyer, and the *acceptance* is made by the seller, the *sending of the seller's acceptance* is the critical transaction. If acceptance is said to take place when the acceptance is sent, then the [seller's] forum is the relevant jurisdiction, whilst the opposite is true if we conclude that it is actual receipt which forms the contract.

Section 25 of the ETQA addresses *where* an electronic communication is taken to have been dispatched and received, unless otherwise agreed by the sender and recipient of the electronic communication. However, s 25 of the ETQA does not solve the current problem, as it does not state whether it is the place of sending, or the place of receipt of the communication that is the place of formation of a contract (Hill 2001, pp53-4).

It is therefore apparent that when a contract has been formed electronically, it may be difficult to determine the place where the contract was formed. However, in the context of electronic construction contracts, contracts of this magnitude will invariably contain a clear provision whereby the parties agree to submit to the jurisdiction of the courts of a particular forum, and to the applicable law that will govern the contract. Where the choice of law and jurisdiction is clearly specified and has a logical connection with the contract, it is highly unlikely that a court would disturb the agreement that has been reached by the parties on this issue.

3.7.1 Conclusion

Although it may be difficult to determine the actual place where an electronic construction contract has been formed, this problem will have minimal legal relevance where an appropriate jurisdiction and governing law clause is incorporated into the construction contract.

3.8 Attribution of electronic communications – authority to contract

In an electronic environment, it will be important to authenticate the identity of the sender of an electronic communication. Section 5.3.9 of this Report deals with the various security measures that may be adopted to effectively authenticate a person's identity.

In the context of electronic contract formation, it will also be important to ensure that a party who purports to enter into a contractual relationship via electronic communications is authorised to enter into the contract. This issue is touched upon by s 26 of the ETQA. It provides as follows:

> **26 Attribution of electronic communications**
>
> (1) For a State Law, unless otherwise agreed between the purported originator of an electronic communication and the addressee of the communication, the purported originator of the communication is bound by the communication only if it was sent by the purported originator or with the purported originator's authority.
>
> (2) Subsection (1) does not limit a State law that provides for:
>
> (a) conduct engaged in by a person within the scope of the person's actual or apparent authority to be attributed to another person; or
>
> (b) a person to be bound by conduct engaged in by another person within the scope of the other person's actual or apparent authority.

In the context of forming electronic construction contracts, this means that a ‘purported originator’ will only be bound by:

- an electronic offer to enter into a contract; or
- an electronic acceptance of an offer,

if the purported originator sends the offer or acceptance themselves, or if the person who sends the relevant communication on their behalf was authorised to do so.

Section 26 of the ETQA is not controversial, as it does not change the operation of existing agency laws or the provisions of the *Corporations Act 2001* (Cth), that determine when a person or company will be bound by a contract. If a person who sends an offer or acceptance communication has actual or apparent authority to bind the ‘purported originator’, or (in the case of companies only), they can be assumed to have such authority under the *Corporations Act 2001* (Cth), then the ‘purported originator’ will be bound by the communication.

Accordingly, the fact that a construction contract may be formed by electronic communications does not alter the existing laws that determine whether a person is authorised to enter into a contractual relationship on behalf of another person or entity. In an electronic environment, it has been noted that some interesting litigation may potentially arise where, for example, a message has not been sent by the purported originator but by someone else with access to their systems and password (Lawrence 2000, p91). However, the resolution of such issues would still be conducted under existing legal principles.

3.8.1 Conclusion

Regardless of whether a construction contract is formed electronically or through paper based communications, the legal principles that determine whether a person is authorised to enter into a contractual relationship on behalf of another person or entity remain the same.

3.9 Mistake in the formation of electronic contracts

Where a fundamental mistake has been made at the time of contract formation by either one or both contracting parties, there are certain established rules under our common law, and also equitable principles that may enable the contract to be set aside as a consequence of the mistake. These principles will apply regardless of whether the contract has been formed through paper based or electronic communications.

Under Australian law, a review of the literature does not reveal any additional legal issues in the area of mistake that would arise from a construction contract being formed in an electronic as opposed to paper based environment. Neither the ETQA nor the Commonwealth *Electronic Transactions Act 1999* (Cth) change the common law and equitable principles that apply where a mistake has been made in the formation of a contract.

The fact that electronic communications may take place quickly and can even be automated, increases the risk that mistakes may be made which cannot readily be corrected before a recipient of a communication relies on the mistake (Hultmark Ramberg 2001, p20). Accordingly, other jurisdictions have implemented provisions that address the issue of mistake in an electronic environment, with a particular focus on mistakes that take place when an individual makes an input error when dealing with the automated message system of another party. An example of such a provision can be found in Article 14 of the UN Convention on the Use of Electronic Communications in International Contracts.

Section 10 of the United States *Uniform Electronic Transactions Act 1999* (‘UETA’) also addresses the situation where an error has been made by an individual when conducting an automated transaction, but goes even further. The UETA also regulates the position where the parties have agreed to use a security procedure to detect changes or errors in an electronic record, and a change or error is not detected by a party because they failed to adhere to the agreed security procedure. In this situation, the UETA allows the party who has used the agreed security procedure to avoid the effect of the changed or erroneous electronic record.

3.9.1 Conclusion

Where a mistake has been made during the formation of a construction contract, the same legal principles will apply irrespective of whether the contract has been formed electronically, or through paper based communications. Where the parties intend to administer their construction contract within an electronic environment, it may be advisable for them to implement communication protocols in an attempt to minimise the occurrence of inadvertent mistakes in the contract administration process.

3.10 Statutory requirements for contracts to be in writing

3.10.1 General introduction

Where a construction contract incorporates a guarantee and has been formed by electronic communications, the question that arises is whether the guarantee is 'in writing', and is therefore enforceable by the courts.

Under general law contractual principles, there is no particular requirement for a contract to be formed in writing. However, in most jurisdictions in Australia there are legislative requirements for certain types of contracts to be in writing, including land contracts and guarantees. These types of provisions are designed to prevent the perpetration of fraud and are remnants of the original English Statute of Frauds 1677. Equivalent legislation exists in most common law countries including, for example, the United States, New Zealand and Singapore.

In Queensland, under s 56(1) of the *Property Law Act 1974* (Qld) a guarantee is only enforceable if it is in writing. This section states:

> No action may be brought upon any promise to guarantee any liability of another unless the promise upon which such action is brought, or some memorandum or note of the promise, is *in writing*, and signed by the party to be charged, or by some other person by the party lawfully authorised. [emphasis added]

A review of the literature reveals an abundance of academic commentary on the ability of electronic communications to satisfy statutory writing requirements. Although there is little Australian case law on the issue, international cases from the United States, the United Kingdom and Singapore provide helpful assistance on the matter. In an Australian context, the issue must be analysed from two perspectives:

- The position under the ETQA must be considered.
- As the literature reveals doubts about the effectiveness of the ETQA to resolve the issue, and in certain circumstances the ETQA may not even apply, the position under general law contractual principles must be addressed.

3.10.2 *Electronic Transactions (Queensland) Act 2001* (Qld)

Section 11 of the ETQA purports to allow requirements of writing to be satisfied by electronic communications. Section 11 of the ETQA provides:

> **11 Requirement to give information in writing**
>
> (1) If, under a State law, a person is required to give information in writing, the requirement is taken to have been met if the person gives the information by an electronic communication in the circumstances stated in subsection (2).

(2) The circumstances are that -

(a) at the time the information was given, it was reasonable to expect the information would be readily accessible so as to be useable for subsequent reference; and

(b) the person to whom the information is required to be given consents to the information being given by an electronic communication.

The operation of s 11 is impacted upon by certain terms that are defined within the ETQA. The relevant defined terms include:

> **'State law**' is defined to mean: '(a) any law in force in the State, whether written or unwritten; or (b) any instrument made or having effect under a law mentioned in paragraph (a)' (Schedule 2 ETQA).
>
> '**give information**' is defined to include, but is not limited to, the following – '(a) make an application; (b) make or lodge a claim; (c) give, send or serve a notification; (d) lodge a return; (e) make a request; (f) make a declaration; (g) lodge or issue a certificate; (h) make, vary or cancel an election; (i) lodge an objection; (j) give a statement of reasons.' (s 10 ETQA)
>
> **'electronic communication'** is defined to mean – '(a) a communication of information in the form of data, text or images by guided or unguided electromagnetic energy; or (b) a communication of information in the form of sound by guided or unguided electromagnetic energy, if the sound is processed at its destination by an automated voice recognition system.' (Schedule 2 ETQA)
>
> **'consents'** is defined to include 'consent that can reasonably be inferred from the conduct of the person concerned, but does not include consent given subject to conditions unless the conditions are complied with.' (Schedule 2 ETQA).

In the context of an electronic construction contract that contains a guarantee, the literature and case law identifies the following issues when relying on s 11 of the ETQA to establish that the guarantee is 'in writing':

- **Commencement:** The ETQA (and other associated electronic transactions legislation in Australia) will not apply to a transaction that takes place before the legislation came into operation (*McGuren v Simpson* [2004] NSWSC 35). Accordingly, to obtain the benefit of the legislation, the contract must have been formed on or after the date that the legislation commenced.

  (The Commonwealth *Electronic Transactions Act 1999* (Cth) commenced on 15 March 2000; most of the ETQA commenced on 1 November 2002; the *Electronic Transactions Act 2000* (NSW) commenced on 30 November 2001; the *Electronic Transactions (Victoria) Act 2000* (Vic) commenced on 1 September 2000; the *Electronic Transactions Act 2000* (Tas) commenced on 1 June 2001; the *Electronic Transactions (Northern Territory) Act 2000* (NT) commenced on 13 June 2001; the majority of the *Electronic Transactions (Australian Capital Territory) Act 2000* (ACT) commenced on 1 July 2001; the *Electronic Transactions Act 2000* (SA) commenced on 1 November 2002; and the *Electronic Transactions Act 2001* (WA) commenced on 2 May 2003).

- **A requirement for writing**: Section 56(1) of the *Property Law Act 1974* (Qld) does not actually *require* a guarantee (or relevant note or memorandum of the promise) to be 'in writing'. Instead, the legislation simply provides that the guarantee will not be enforceable (Nikolich 2003, p31). It has been suggested that this issue may be resolved by interpreting a requirement to give information in writing, to include a provision that sets out consequences for an absence of writing (Christensen, Duncan & Low 2002, p61).

  Section 56(1) of the *Property Law Act 1974* (Qld) may be contrasted with Article 9(2) of the UN Convention on the Use of Electronic Communications in International Contracts.

This article refers to where the law requires a communication or contract to be in writing, or where the law provides consequences for the absence of writing. It is also relevant to note that in Victoria, the legislation that says an unwritten guarantee is not enforceable also specifically says that the writing requirement may be met in accordance with the relevant electronic transactions legislation (for example, s 126 *Instruments Act 1958* (Vic)).

- **Giving information in writing:** It has been argued that as s 11 of the ETQA only applies where a State law requires a person to 'give information' in writing, the section may not apply to the formation of a contract of guarantee, as this is very different to the situation where a law actually requires a person to provide information (Christensen, Duncan & Low 2002, p60). Although the ETQA definition of 'give information' is not exhaustive, none of the actions contained in the definition remotely relate to the formation of a contract. Accordingly, it has been suggested that it is uncertain whether the ETQA permits the conclusion of a contract of guarantee in electronic as opposed to written form (Nikolich 2003, p31).

- **Consent:** In establishing that s 11 of the ETQA applies to a guarantee, it is important to show that the counterparty to the transaction has consented to the information being provided electronically. It is clear from the definition of 'consent' in the ETQA that consent may be express or implied from conduct. It is generally uncertain when conduct may be construed as the giving of consent. It has been argued that although consent is unlikely to be implied simply because a person has previously used electronic communications, consent may very well be inferred where the parties have previously conducted similar transactions electronically (Nikolich 2003, p29).

  Some commentary has also suggested that the requirement for consent may actually inhibit the use of electronic communications. As the circumstances in which consent may be implied are not defined in the legislation, contracting parties may choose to adopt a cautious approach and continue to send communications that are legally certain (Nicoll 2000, p200). In essence, the requirement for consent has been said to raise more questions than answers (Nicoll 2000, p204).

- **Accessibility for subsequence reference:** For the ETQA to apply, at the time the information was given, it must have been reasonable to expect the information would be readily accessible so as to be useable for subsequent reference. It has been suggested that this requirement would be satisfied if the contracting parties store the information such that it is able to be later accessed, retrieved and read (Christensen, Duncan & Low 2002, p61).

- **The ETQA general rule:** If s 11 of the ETQA does not apply to a guarantee that has been formed by electronic communications, then it may be argued that the general rule contained in s 8 of the ETQA will apply with the consequent effect that the guarantee is still valid. Under s 8 of the ETQA, a transaction is not invalid under a State law merely because it took place wholly or partly by electronic communications. However, it may be argued that s 8 cannot apply as there is no State law that has the effect of invalidating the guarantee – s 56 of the *Property Law Act 1974* (Qld) does not invalidate the guarantee, it simply means that the guarantee will not be enforced by a court.

Faulks v Cameron (2004) 32 Fam LR 417 is the only judicial decision that has considered the application of the Australian electronic transactions legislation to a statutory requirement for an agreement to be in writing. However, the court did not devote any time to the consideration of whether the emails in that case constituted 'writing' under the *Electronic Transactions (Northern Territory) Act 2000* (NT). In fact, the court did not even refer to the equivalent writing provision contained in s 8 of the Northern Territory Act. In essence, the decision appeared to presume that printed emails constituted writing, and was more concerned with resolving the question of whether a type-written signature on an email meant that the relevant agreement had been ‘signed’.

As there has been little judicial consideration of how s 11 of the ETQA may apply to a guarantee that has been formed by electronic communications, and the literature reveals a number of issues with this provision, the application of s 11 of the ETQA remains unclear. It is therefore necessary to consider the position under general law contractual principles.

3.10.3 General law contractual principles

If the ETQA does not apply to a guarantee that has been formed by electronic communications, the question to be resolved is whether general law contractual principles will recognise that the guarantee is ‘in writing’ for the purposes of s 56 of the *Property Law Act 1974* (Qld).

The only judicial determination in Australia about whether general law principles allow electronic communications to satisfy a statutory writing requirement is the case of *McGuren v Simpson* [2004] NSWSC 35. This case considered whether an email was capable of constituting an acknowledgment ‘in writing’ for the purposes of the *Limitation Act 1969* (NSW), as the relevant defendant in the case was able to produce a printed email sent to him by the plaintiff. In holding that the *Limitation Act 1969* (NSW) should be construed to accommodate technological changes and that the email amounted to a written document, Harrison M relied on the following authorities (at [19] to [20]):

- The English decision of *Lockheed-Arabia v Owen* [1993] 3 All ER 641 held that a photocopy of a cheque amounted to ‘writing’ for the purposes of the *Acts Interpretation Act 1978* (UK). In reaching this decision, Mann LJ rationalised that ‘An ongoing statute ought to be read so as to accommodate technological change’ (at p 646).

- In the United States, the case of *Wilkens v Iowa Insurance Commissioner* (1990) 457 NW 2d 1 (Iowa 1990) held that a statutory requirement to keep a written record of a contract was satisfied by the records being kept on a computer system.

- Reliance was also placed on academic commentary to the effect that a document which may be printed and stored amounts to a document that is ‘in writing’.

The fact that a printed email will constitute ‘writing’ for the purposes of a Statute of Frauds writing requirement is supported by decisions in other jurisdictions:

- United States of America - *Dow Chemical Company v G.E.,* 2005 US Dist. LEXIS 40866 (E.D. Mich. 2005); *Bazak International Corp v Tarrant Apparel Group,* 2005 US Dist. LEXIS 14674 (S.D.N.Y 2005); *International Casings Group Inc. v Premium Standard Farms Inc,* 2005 US Dist. LEXIS 3145 (W.D. Mo 2005); *Lamle v Mattel Inc.,* 2005 US App LEXIS 217 (Fed. Cir. 2005); *Roger Edwards LLC v Fiddes & Sons,* 245 F.Supp. 2d 251 (D. Me. 2003); *Rosenfeld v Zerneck,* 4 Misc. 3d 193, 776 N.Y.S.2d 458, 2004 N.Y. Misc. LEXIS 497 (2004); *Cloud Corporation v Hasbro Inc.,* 314 F. 3d 289 (7th Circ. Ill 2002); *Shattuck v Klotzbach* 14 Mass. L. Rep 260 (Mass. Super. Ct. 2001).

- Singapore – *SM Integrated Transware Pty Ltd v Schenker Singapore (PTE) Ltd* [2005] 2 SLR 651.

Accordingly, under general law principles it appears relatively clear that the printed form of an electronic document will be sufficient to satisfy the requirement of s 56 of the *Property Law Act 1974* (Qld) for a guarantee to be in writing.

However, the literature has moved on to consider whether a purely electronic document which never takes physical form may also constitute ‘writing’. As noted by Kidd and Daughtrey (2000, p126):

> While a printed copy of a contract formed electronically is identical to any other 'pen and paper' writing, the less certain case involves 'paperless' electronic contracts that exist only in computer memories or on computer screens.

Purely electronic communications

In the context of guarantees and s 56 of the *Property Law Act 1974* (Qld), whether a purely electronic document may constitute 'writing' may depend upon the definition of 'writing' contained in the *Acts Interpretation Act 1954* (Qld). This definition will apply to any construction of s 56 of the *Property Law Act 1974* (Qld).

Under s 36 of the *Acts Interpretation Act 1954* (Qld) 'writing' is defined to include 'any mode of representing or reproducing words in a *visible* form' (emphasis added). There are several competing arguments about whether a purely electronic document may satisfy this concept of 'writing'. The various arguments include:

- This definition of 'writing' may be satisfied if the contract is capable of retrieval and reproduction in a visible form, regardless of whether the document is ultimately printed and reduced to physical form (Christensen, Duncan & Low 2002, p44).

- In the context of a similar legislative definition in the Canadian *Interpretation Acts*, the Canadian Department of Justice has indicated that the definition suggests that a message does not have to be reduced to paper form to constitute 'writing', particularly in light of the courts' willingness to adapt to new technology (Department of Justice Canada 2005, pp9-5 to 9-6).

- Some commentators have suggested that an electronic document is not 'writing' because '…digital information is a series of electronic bits in a chip or some other recording medium. It is not a visible representation or reproduction of words' (Christensen & Low 2003, p417). For example, in the context of the English definition of 'writing' contained in the *Interpretation Act 1978* (UK) (which is similar to the definition in Queensland) Edwards and Waelde (1997, p139) argue that:

  > A document which exists solely in digital form, for example an electronic mail message stored on the hard disk of the recipient's computer, will not be capable of coming within this definition as the electronic impulses representing its contents are not visible.

- In contrast to the previous argument, the Law Reform Commission for England and Wales notes that electronic communications have a dual form – the display on the screen and the transmitted/stored form as files of binary (digital) information. The Commission argues that it is the screen display rather than the binary information itself that constitutes the 'writing' (Beale & Griffiths 2002, pp471-2).

There is very little judicial guidance on whether a completely electronic document may satisfy a writing requirement, largely due to the fact that where emails have been produced as evidence, they have been produced in printed form. However, certain judicial comments may provide a useful basis to predict the possible future development of the law in a wholly electronic environment.

For example, in the United States decision of *Bazak International Corp v Tarrant Apparel Group,* 2005 US Dist. LEXIS 14674 (S.D.N.Y 2005) the court was concerned with whether or not emails could satisfy a writing requirement under the Uniform Commercial Code ('UCC'). The UCC defined 'written' or 'writing' to include 'printing, typewriting or any other intentional reduction to *tangible* form [emphasis added]'. Although the emails were produced as printed evidence, Marrero USDJ made the following comments about the intangible nature of emails:

> Although e-mails are intangible messages during their transmission, this fact alone does not prove fatal to their qualifying as writings under the UCC. Aside from posted mail, the forms of

> communication regularly recognized by the courts as fulfilling the UCC "writing" requirement, such as fax, telex and telegraph, are all intangible forms of communication during portions of their transmission. Just as messages sent using these accepted methods can be rendered tangible, thereby falling within the UCC definition, so too can e-mails…Additionally, because "under any computer storage method, the computer system 'remembers' the message even after being turned off", whether or not the e-mail is eventually printed on paper or saved on the server, it remains an objectively observable and tangible record that such a confirmation exists… Consequently, there appears to be little distinction between e-mails and other forms of communication regularly recognized under the Statute as adequate "writings". (at pp383-384).

Some academic commentary on the United States UCC appears to support these judicial comments. For example, it has been suggested that even if an email is not printed, it still exists as data 'stored on an internal computer drive, a floppy diskette or a magnetic tape.' Accordingly, the email still has a 'definite tangible form that can be converted to readable format relatively easily and may actually constitute more durable evidence of a contract than paper can provide' (Huey 2003, p704). When comparing the UCC definition of 'writing' to the definition contained in the Queensland *Acts Interpretation Act 1954* (Qld), it is apparent that the UCC defines writing by reference to 'tangible form' whereas the Queensland definition refers to 'visible form'. It could therefore be argued that if an unprinted email is capable of being considered in 'tangible form', then it should be able to satisfy the possibly lower benchmark requirement of being in 'visible form'.

Ultimately, whether or not an unprinted electronic communication can be said to be 'in writing' is unclear and further research on the issue is warranted.

3.10.4 Conclusion

It is uncertain whether s 11 of the ETQA can be relied upon to establish that a guarantee that has been formed by electronic communications satisfies the statutory requirement for a guarantee to be in writing. Under the general law, if an electronic communication is printed, the weight of authority suggests that the printed communication will satisfy a statutory writing requirement.

The law is unclear on the position of purely electronic documents. It is therefore possible that a guarantee which exists in a purely electronic format may not be enforceable because it does not meet the writing requirements of s 56 of the *Property Law Act 1974* (Qld).

3.11 Acceptance of an offer that requires acceptance to be communicated in writing

3.11.1 General introduction

As previously noted, under general law contractual principles there is no particular requirement for a contract to be formed in writing. However, problems may arise where an offer is made to a party to form a construction contract, and the offer specifically requires that acceptance be communicated in writing.

The question that must be resolved is whether an electronic acceptance of the offer is valid. Once again, as there are doubts as to whether or not the ETQA resolves the issue, the problem must be considered by reference to both the ETQA and general law contractual principles.

3.11.2 *Electronic Transactions (Queensland) Act 2001* (Qld)

The following sections of the ETQA may be relevant to this issue:

- s 11 ETQA - relating to requirements under State laws to give information in writing (as reproduced in section 3.10.2 of this Report);

- s 12 ETQA - relating to permissions under State laws to give information in writing (Section 12 is in similar terms to s 11 of the ETQA); and

- s 8 ETQA – this section generally establishes that transactions (including contracts and agreements) are not invalid under a State law merely because they take place wholly or partly by one or more electronic communications. This general rule can be displaced by more specific provisions that are contained in Chapter 2 of the ETQA.

A review of the literature reveals a number of arguments to suggest that where an offer specifically requires an acceptance to be communicated in writing, the ETQA may not be effective to validate an electronic communication of acceptance. The following arguments have been raised in relation to the ETQA:

- **Giving information in writing:** The ETQA contains an inclusive definition of what it means to 'give information' (s 10 ETQA). The instances that are listed in the definition do not resemble the acceptance of a contract, and it has been argued that the very concept of 'information' is different to the expression of a will to be bound by an agreement. Although the definition of what it means to 'give information' is not exhaustive, it may be ambitious to argue that the concept extends to exchanges between parties that bring about the formation of a contract (Sheridan & Rigotti 2001, pp48-9). Accordingly, the concept of 'giving information' appears to be directed towards the notification of information to a person, rather than extending to contract formation (Christensen, Duncan & Low 2002, p60).

  On the basis of these arguments, ss 11 and 12 of the ETQA would not apply to an electronic communication of acceptance.

- **State law:** Sections 11 and 12 of the ETQA only apply where it is a 'State law' that permits or requires information to be given in writing. It is clear that the concept of a 'State law' embraces not only statutes that have been enacted by Parliament, but also general law contractual principles. However, in the situation at hand, it is the contractual offer by the offeror which requires acceptance to be communicated in writing, rather than a requirement or a permission under a statute or the general law.

  Accordingly, it may be argued that ss 11 and 12 of the ETQA cannot apply, as there is no relevant 'State law' that requires or permits the giving of information in writing. However, in direct opposition to this argument, it may still be contended that a contractual offer requiring acceptance to be communicated in writing does constitute a requirement under a 'State law', as the general law would require a valid acceptance of the offer to be communicated in writing.

- **Consent and accessibility for subsequence reference:** Even if there is scope for ss 11 or 12 of the ETQA to apply to an electronic acceptance in these circumstances, it must also be established that the offeror consented to the acceptance being given electronically, and that when the acceptance was given it was reasonable to expect that it would be readily accessible so as to be useable for subsequent reference.

- **The ETQA general rule:** If ss 11 and 12 of the ETQA do not apply, then s 8 of the ETQA must be considered. This section generally provides that the agreement would not be invalid merely because it has taken place wholly or partly by one or more electronic communications. A number of arguments have been raised to suggest that s 8 of the ETQA cannot be relied upon to give effect to an electronic acceptance where the offer specifically requires acceptance to be communicated in writing. The arguments are that:

- This may override the long standing position under the general law that an offeror has the right to decide the mode and manner in which acceptance of the offer must be notified;
- Section 8 of the ETQA does not apply because there is a more general failure to comply with contract law principles that govern offer and acceptance; and
- Section 8 should be interpreted as being subservient to any laws which provide for a result that is contrary to s 8 of the ETQA, including the general laws that govern contract formation (Sheridan & Rigotti 2001, p49).

Accordingly, there are arguments to suggest that the ETQA may not have the effect of validating an electronic acceptance of an offer, where the offer expressly requires acceptance to be communicated in writing. Although the case of *Ford v La Forrest* [2001] QSC 261 held that an acceptance sent by email is capable of creating legal relations, the offer in that case did not specify that the acceptance had to be in writing, and email communication had been a common form of communication between the parties in that case. It is therefore essential to consider the position under general law contractual principles.

3.11.3 General law contractual principles

If the ETQA does not apply, the question that arises is whether general law contractual principles will recognise the validity of an electronic acceptance where an offer specifically requires acceptance to be communicated 'in writing'.

Under the general law, the offeror has the ability to stipulate exactly how an acceptance should take place, including the method to be used to communicate acceptance. It has been argued by one commentator that where an offer stipulates that the acceptance must be in writing, then an electronic communication of acceptance would be invalid under general contract law principles (Sheridan & Rigotti 2001, p49). However, there are alternative stronger arguments (outlined below) that suggest this is not necessarily the case.

Firstly, even if a mode of communication has been prescribed, there is some controversy surrounding whether an offeree has to strictly adhere to this requirement (Seddon & Ellinghaus 2002, p134). Although a failure to respond using the specified mode of communication may prevent a contract from being formed, in certain situations this may not be fatal to the formation of a contract (Willmott, Christensen & Butler 2005, p62). For example, where a faster mode of communicating acceptance is used, then it is probable that the acceptance will be effective because the faster mode of communication is to the offeror's advantage (Seddon & Ellinghaus 2002, p134; Willmott, Christensen & Butler 2005, p62). If an offeror has insisted that an acceptance must be sent by a particular method and by that method only, an alternative mode of acceptance would not be effective. However, the language used in the offer would have to be very clear before a court would conclude that the particular mode of acceptance that has been specified is mandatory (Seddon & Ellinghaus 2002, p134).

Secondly, it is questionable whether a requirement for an acceptance to be in writing amounts to designating a particular method for communicating acceptance. While an oral acceptance would obviously not be effective, in accordance with the courts' willingness to construe laws in a way that accommodates technological changes (as detailed in section 3.10 above), it is suggested that if the relevant electronic communication may be printed and reduced to physical form, this may satisfy the requirement that the acceptance be 'in writing'. Accordingly, it is probable that even if an offer requires an acceptance to be communicated in writing, this may be satisfied by an electronic communication of acceptance if the communication may be printed.

The more interesting question to be resolved is whether an electronic communication of acceptance which never takes physical form may also constitute an acceptance that is ‘in writing’. The analysis on this point would be similar to the discussions on this issue contained in section 3.10 above. Ultimately, the legal position on this issue remains unclear.

3.11.4 Conclusion

It is unclear whether ss 11, 12 or 8 of the ETQA can be relied upon to establish that an electronic communication of acceptance is effective where the offer requires acceptance to be communicated in writing. Further guidance on this issue will only be obtained by subsequent decisions of the courts.

Under the general law, if an electronic communication of acceptance may be printed and reduced to physical form, it is probable that the acceptance would be effective. However, there is no absolute certainty on this point and whether or not a valid contract has been formed would very much depend upon the precise terms of the offer, and indeed, whether or not the offer was communicated to the offeree in electronic form. In the case of a purely electronic acceptance, it is uncertain whether the acceptance would be valid as the legal position on this issue remains unclear.

3.12 Statutory requirements for contracts to be signed

3.12.1 General introduction

Where an electronic construction contract incorporates a guarantee, the further question that arises is whether the guarantee is ‘signed’, and is therefore enforceable by the courts.

Under general law contractual principles, there is no particular requirement for a contract to be signed. Accordingly, for the majority of contracts no hand-written or other form of signature is required for a contract to be valid and binding. However, as outlined in section 3.10 above, s 56(1) of the *Property Law Act 1974* (Qld) requires a guarantee (or some memorandum or note of the promise) to be ‘signed’ in addition to being ‘in writing’.

Before considering the legal issues that arise in connection with the signing of an electronic contract, it is important to consider the various ways that a party may ‘sign’ an electronic document.

3.12.2 How can an electronic document be signed?

3.12.2.1 Electronic signatures

The term ‘electronic signature’ is usually used to describe signatures incorporated in a document by electronic or cryptographic means. Some examples of electronic signatures include the type-written name of a signatory, the pasting in of a scanned version of the signer's signature, clicking an ‘I Accept’ button, the use of a userid and password, or using cryptographic technology such as digital signatures.

Electronic signatures may identify the person who has appended the signature to the document and (as discussed further below) may indicate the person’s agreement to the content of the document in the same way as a handwritten signature. The examples of electronic signatures listed above (other than digital signatures) are not able to assure both the sender’s identity and the integrity of documents. However, an advantage of these types of signatures is that, in many cases, they are in human readable form and can be easily understood by the humans.

3.12.2.2 Digital signatures

A digital signature is signing technology based on public key cryptography. Public key cryptography involves the use of two keys, a private key and a public key. Each individual in the system has a private key which only they know and they distribute the corresponding public key to the public. When an electronic document is digitally signed a secured cryptographic hash function is used to create a message digest of the original document and the hash value is signed using the private key of the signatory. The output of this signing function is known as a digital signature.

The person who needs to verify a digital signature requires the communicated document, the digital signature and the public key of the person who has signed the document. To verify the signature, the same hash algorithm is run over the communicated document and a verification algorithm using the public key is run over the digital signature. The output of the verification algorithm is compared with the hash value and if they are the same, then the signature is verified as being a valid signature of the holder of the private key and the integrity of the message is confirmed.

If confidentiality is required, the transmitted message and digital signature can be encrypted by the sender of the communication by using the public key of the message recipient. The encrypted message and digital signature are then transmitted and may be decrypted by the recipient through the use of their own private key.

3.12.3 *Electronic Transactions (Queensland) Act 2001* (Qld)

Section 14 of the ETQA is designed to allow signature requirements to be met in the context of electronic communications. Under this provision, if a State law requires a person's signature, this requirement is met for an electronic communication if the following three conditions are satisfied:

- a method is used to *identify* the person and to indicate the person's *approval* of the information communicated (ie, the 'method' would be an electronic or digital signature);

- having regard to all relevant circumstances when the method was used, the method was *as reliable as was appropriate* for the purposes for which the information was communicated; and

- the person to whom the signature is required to be given has *consented* to the requirement being met by using the method.

The only Australian decision that has considered the effectiveness of an electronic signature under Australia's electronic transactions legislation is the decision in *Faulks v Cameron* (2004) 32 Fam LR 417. This decision involved emails that ended with the type-written words 'Regards Angus' and 'Regards Angus Cameron'. The court had to determine whether the emails were 'signed' as a consequence of the *Electronic Transactions (Northern Territory) Act 2000* (NT) (which contains a provision almost identical to s 14 of the ETQA). With surprisingly little analysis, it was held that the emails had been signed. Young AM was satisfied that:

> …the printed signature on the defendant's emails identifies him and indicates his approval of the information communicated, that the method was reliable as was appropriate and that the plaintiff consented to the method. I am satisfied that the agreement is 'signed'… (at page 426).

Although this decision suggests that the ETQA easily allows even the most basic form of electronic signature to satisfy a statutory signing requirement, a review of the literature identifies a number of issues that may arise with s 14 of the ETQA:

- **Commencement:** As previously mentioned, the ETQA (and other associated uniform electronic transactions legislation in Australia) will not apply to a transaction that takes place before the legislation came into operation (*McGuren v Simpson* [2004] NSWSC 35).

- **A requirement for a signature:** As discussed in section 3.10 above, s 56(1) of the *Property Law Act 1974* (Qld) does not actually *require* a guarantee to be signed - it simply provides that if the guarantee is not signed it will not be enforceable. Section 14 of the ETQA will only apply if a State law can be said to *require* a person's signature. However, this issue may be circumvented by broadly interpreting the word 'require' to include the situation where a failure to have a signature results in adverse consequences (Christensen, Duncan & Low 2002, p71).

  The decision in *Faulks v Cameron* (2004) 32 Fam LR 417 supports the argument that a broad interpretation should be adopted when determining if a State law 'requires' a signature to be provided. The legislation in that case (the *De Facto Relationships Act 1991* (NT)) did not specifically require the relevant agreement to be signed – it simply provided that if the court was satisfied that the agreement was in writing and signed, then the court could not make an order that was inconsistent with the terms of the agreement. As the court was prepared to apply an equivalent electronic signing provision in s 9 of the *Electronic Transactions (Northern Territory) Act 2000* (NT), by implication the court was satisfied that the *De Facto Relationships Act 1991* (NT) could be said to 'require' the giving of a signature.

  Section 56(1) of the *Property Law Act 1974* (Qld) may be contrasted with provisions in other jurisdictions. For example, article 9(3) of the UN Convention on the Use of Electronic Communications in International Contracts refers to a law that either requires a communication or contract to be signed by a party, or provides for consequences for the absence of a signature.

- **Identification and approval:** Under s 14 of the ETQA, the signature method used does not have to verify the integrity of the information sent in an electronic communication, it need only identify the person and indicate their approval of the information communicated. *Faulks v Cameron* (2004) 32 Fam LR 417 indicates that a simple electronic signature may, depending upon the circumstances, be sufficient to *identify* the person and to indicate the person's *approval* of the information communicated. It has been suggested that both electronic signatures, and the more secure method of digital signatures would satisfy this requirement of the ETQA (Christensen, Duncan & Low 2002, p72).

- **Reliability and appropriateness of the signature method:** The reliability of the signature method used is the crucial issue under the ETQA. In the context of establishing that a particular signature method is reliable, the ETQA does not prescribe that any particular form of technology be used. Clause 10 of the Revised Explanatory Memorandum to the Commonwealth *Electronic Transactions Bill 1999* (Cth) notes that this is a deliberate decision so that the legislation does not have to be amended to take into account technological changes and that '…it is more appropriate for the market to assess appropriate signature products for their particular purposes rather than have legislation specify acceptable technologies.'

  It has been argued that this creates uncertainty and that parties may be unable to make an assessment of which method is appropriate for use on a transaction by transaction basis (De Zilva 2003, p1016). Accordingly, there is a risk that a particular signature method may not be considered reliable or appropriate in the context of a particular transaction. This is especially the case as the courts have yet to consider the meaning of the words 'as reliable as was appropriate' (Davidson 2004, p30).

  Although reliability is assessed at the time the signature method is used (as opposed to at a later date), the literature suggests that there is still much scope for disagreement and litigation after the fact about whether a particular signature method chosen was in fact reliable and appropriate, and that when taken to the extreme, this provision may potentially exclude all forms of electronic signatures on the basis that no method was sufficiently reliable (Lawrence 2000, pp89-90). It has been suggested that the critical factors that may impact upon reliability is the ability of the signature method to authenticate the document, and to maintain the integrity of the document for later reference (Christensen, Duncan & Low 2003, p12).

> The 'reliability' requirement in the ETQA is similar to a provision contained in Article 7 of UNCITRAL's Model Law on Electronic Commerce 1996. The Guide to Enactment of this Model Law lists approximately 14 legal, technical and commercial factors that may be taken into account when determining whether a signature method is reliable and appropriate. To alleviate the uncertainties surrounding this issue, commentators have called upon the legislature to incorporate into the ETQA more specific criteria on the types of signatures that may be considered to be effective, as has been done in the European Union Directive on Electronic Signatures (Article 2(2)) (Christensen, Duncan & Low 2002, p74).

- **Consent:** For s 14 of the ETQA to apply to a guarantee, the person to whom the signature is required to be given, must have consented to the signature requirement being met by the use of the relevant signature method. A requirement for consent applies to a number of the ETQA provisions, and absent the existence of express consent it is generally uncertain when conduct may be construed as the giving of consent. It has been suggested that the legislature must clarify the meaning of 'consent' (De Zilva 2003, pp1018-19).

> In the context of signatures, consent must be given to 'the method' used to satisfy the signature requirement. It has been suggested that proper 'consent' in this context may be narrower than a simple consent to the use of electronic communications (Christensen, Duncan & Low 2002, p73).

Accordingly, it appears that s 14 of the ETQA may potentially be relied upon to establish that a guarantee that has been signed with an electronic or digital signature has been sufficiently 'signed' for the purposes of the *Property Law Act 1974* (Qld), and is therefore enforceable. However, the main difficulties that would need to be considered and addressed under the ETQA are:

- Establishing that consent has been given to the use of the signature method – for the avoidance of doubt, consent should be expressly given.

- Establishing that having regard to all relevant circumstances at the time the signature method was used, the method of signing was as reliable as was appropriate for the purposes for which the information was communicated. Although it is difficult to predict how this criterion might be satisfied and the approach that a court may take to the issue, from an evidentiary viewpoint there may be some benefit to including within the terms of the contract an agreement between the parties that the signature method which has been adopted is considered by both the parties to be reliable and appropriate in the circumstances and at the time of the transaction. It should be noted, however, that such a provision would not preclude a court from making its own assessment of the appropriateness of the signature method that has been used.

A large number of countries around the world have now implemented legislation that enables an electronic or digital signature to satisfy laws that require a signature to be provided. For example, in the United States many States have now passed legislation to implement a Uniform Electronic Transactions Act. Although the Uniform Electronic Transactions Act is clearly not identical to the ETQA, it is salient to note that in the United States it has been held that based upon this legislation, a type-written name at the bottom of an email, and even the header of an email with the name of the sender may be a sufficient signature to satisfy a Statute of Frauds requirement for an agreement to be signed (for example, *International*

Casings Group Inc. v Premium Standard Farms Inc, 2005 US Dist. LEXIS 3145 (W.D. Mo 2005)).

3.12.4 General law principles

If s 14 of the ETQA cannot be relied upon (because, for example, there has been no consent to the use of an electronic or digital signature), it is essential to ascertain whether the general law will recognise that a guarantee that has been authenticated by either an electronic or digital signature, has been 'signed' for the purposes of s 56 of the *Property Law Act 1974* (Qld).

In the United States, there is a long line of authorities that has held that a type-written name in an email is capable of satisfying a Statute of Frauds requirement for an agreement to be signed: - *Dow Chemical Company v G.E.,* 2005 US Dist. LEXIS 40866 (E.D. Mich. 2005); *Bazak International Corp v Tarrant Apparel Group,* 2005 US Dist. LEXIS 14674 (S.D.N.Y 2005); *Lamle v Mattel Inc.,* 2005 US App LEXIS 217 (Fed. Cir. 2005); *Roger Edwards LLC v Fiddes & Sons,* 245 F.Supp. 2d 251 (D. Me. 2003); *Rosenfeld v Zerneck,* 4 Misc. 3d 193, 776 N.Y.S.2d 458, 2004 N.Y. Misc. LEXIS 497 (2004); *Cloud Corporation v Hasbro Inc.,* 314 F. 3d 289 (7th Circ. Ill 2002); *Shattuck v Klotzbach* 14 Mass. L. Rep 260 (Mass. Super. Ct. 2001).

In Singapore, it has also been held that a type-written name and even the name of a sender in the header of an email is sufficient to satisfy a Statute of Frauds requirement for a signature: *SM Integrated Transware Pty Ltd v Schenker Singapore (PTE) Ltd* [2005] 2 SLR 651. In England, in the context of an agreement that required any variations to be in writing and signed by the parties, it was held that type-written names at the foot of email communications amounted to a sufficient signature – *Hall v Cognos Ltd* (Industrial Tribunal Case No. 1803325/97). In contrast, in the decision of *Nilesh Mehta v J Pereira Fernandes S.A.* [2006] EWHC 813 (Ch) it was found that the automatic insertion of a party's email address at the beginning of an email message did not constitute a signature for the purposes of the Statute of Frauds.

The only judicial determination in Australia about whether general law principles allow an electronic signature to satisfy a statutory signing requirement is the case of *McGuren v Simpson* [2004] NSWSC 35. This case considered whether an email was capable of constituting an acknowledgment in writing and 'signed' for the purposes of the *Limitation Act 1969* (NSW), as the defendant in the case was able to produce a printed email sent to him by the plaintiff, which contained the plaintiff's type-written name. In holding that this constituted a sufficient signature, the court applied a doctrine known as the 'authenticated signature fiction'. This doctrine may be explained as follows:

> Where the name of the party to be charged appears on the alleged note or memorandum, for example, because it has been typed in by the other party, the so-called 'authenticated signature fiction' will apply where the party to be charged expressly or impliedly acknowledges the writing as an authenticated expression of the contract so that the typed words will be deemed to be his or her signature. This principle has no application to a document which is not in some way or other recognisable as a note or memorandum of a concluded agreement. (at [22])

As the plaintiff's name appeared in the email and the email contained an authenticated expression of a prior agreement, the email was found to be a note of a concluded agreement and in effect, the plaintiff's type-written name was deemed to be a signature.

A possible difficulty with relying on *McGuren v Simpson* [2004] NSWSC 35 to argue that an electronic signature will be sufficient in all cases, is that for the authenticated signature fiction to apply, the signatory must have expressly or impliedly indicated that he or she recognises the writing that contains their name, as being an expression of the will to contract (Christensen, Duncan & Low 2002, p3). The decisions of the courts indicate that the authenticated signature fiction may be relied upon for certain types of contracts, however the various States and Territories of Australia have not adopted a uniform approach to the issue and there is yet to be a decision that has applied the authenticated signature fiction to a guarantee. Accordingly, notwithstanding the United States decisions (as discussed above), there may be uncertainty as to the approach that an Australian court will adopt in connection with guarantees.

In the case of digital signatures, there have been no judicial decisions in any jurisdiction that address whether or not a digital signature will satisfy a statutory signing requirement. Accordingly, whether or not a digital signature will be sufficient under Australian law is yet to be determined. It has been suggested that as a digital signature has the potential to fulfil almost all of the traditional functions that are performed by a hand-written signature, a digital signature should be sufficient to satisfy s 56 of the *Property Law Act 1974* (Qld) (Christensen, Duncan & Low 2002, p54). The Law Commission for England and Wales has also argued that the use of a digital signature provides a clear indication that the signatory possessed an authenticating intention. Accordingly, the Commission views the use of a digital signature as satisfying a statutory signature requirement (Beale & Griffiths 2002, pp473-4).

Given the relative ease with which some courts have accepted electronic signatures as satisfying a statutory signing requirement, it may be suggested that the increased security provided by digital signatures should lead to the conclusion that a digital signature will be sufficient. However, until the issue has been determined by the courts, the position with respect to digital signatures remains unclear.

3.12.5 Conclusion

Section 14 of the ETQA may potentially be relied upon to establish that a guarantee that has been signed with an electronic or digital signature has been sufficiently ‘signed’ for the purposes of the *Property Law Act 1974* (Qld). However, the main difficulties that may be encountered when relying upon the ETQA are establishing that:

- consent was given to the use of the signature method; and

- having regard to all relevant circumstances at the time the signature method was used, the signature method was as reliable as was appropriate for the purposes for which the information was communicated.

Until there are further judicial decisions on the application of s 14 of the ETQA, it is difficult to determine how the courts will approach these issues. This is particularly the case with digital signatures, as there has been no judicial consideration of this signature method.

Under the general law, it is uncertain whether an Australian court would hold that an electronic signature is a sufficient signature for the purposes of s 56(1) of the *Property Law Act 1974* (Qld). As the courts are yet to consider digital signatures, the position with respect to digital signatures also remains unclear.

4. ELECTRONIC CONTRACT ADMINISTRATION AND MANAGEMENT

4.1 Overview of issues associated with the electronic administration and management of construction contracts

A review of the relevant literature, legislation and judicial decisions of the courts reveals that the following issues may arise in the electronic administration and management of construction contracts:

- The exchange of electronic communications between parties may, depending upon the terms and conditions of a construction contract, amount to an effective variation of the contract.

- Depending upon the terms and conditions of a construction contract, there may be legal uncertainties about the validity of electronic notices.

- Protocols need to be established to ensure that electronic documents viewed by all construction project participants are identical. It is important that each project participant is using the same software and settings to ensure that all participants view the same document.

- Online collaboration platforms are emerging as the principal tool used in electronic contract administration and management in the construction industry. A range of legal issues may be encountered in relation to the use of collaboration platforms.

4.2 Electronic variations of construction contracts

4.2.1 General introduction

A variation of a construction contract is, in itself, a further contract between the parties. Accordingly, to create a binding agreement to vary a construction contract the five legal elements outlined in section 3.2 above must be present (Willmott, Christensen & Butler 2005, p734). It will also be important to ensure that the persons purporting to enter into the variation agreement are duly authorised to do so (refer to section 3.8 above).

The terms of a construction contract will usually require any variations to the contract to be in writing, and may even require the writing to be signed. Accordingly, absent any provisions in the construction contract that deal with the effectiveness of electronic communications, the question that arises for consideration is whether the construction contract may be effectively varied by an agreement between the parties that takes place via electronic communications. In other words, will an electronic agreement to vary the construction contract constitute an agreement that is in 'writing', and if relevant, 'signed'?

4.2.2 Writing

The analysis of whether or not an electronic variation agreement can be said to be in 'writing' is almost identical to the discussions in section 3.11 (relating to whether or not an electronic communication of acceptance is valid where acceptance is required to be communicated in writing).

Accordingly, until there is further judicial analysis by the courts, it is unclear whether or not the ETQA can be relied upon to establish that an electronic variation agreement is in 'writing'. However, under the general law it is probable that an electronic variation agreement will constitute 'writing' if the electronic communications may be printed and reduced to physical form.

Case law in other jurisdictions supports this conclusion. For example in England, the case of *Hall v Cognos Ltd* (Industrial Tribunal Case No. 1803325/97) considered whether an employment agreement could be effectively varied by email exchanges, when the terms of the employment agreement required any variations to be 'in writing and signed by the parties'. The employee had exchanged various emails with another employee of the company and a company manager in relation to the claiming of travel expenses, which he would not otherwise have been entitled to claim under the terms of his employment agreement. It was argued that the emails did not constitute an effective variation of the employment agreement as the emails were not in writing and signed. This argument was rejected by the tribunal, which was satisfied that:

> …an e-mail is "in writing and signed by the parties" once it is printed out. The position might (it is not necessary to make any finding on this point) be different if the e-mail was only retained temporarily on the computer's hard disk storage system. The documents that were, however, produced from the computer are clearly in writing and bear the signatures of both 'Sarah' and 'Keith'. The fact that those signatures are printed, rather than hand-written, is not in my view material. For those reasons, I reject [the] submission that the relevant e-mail messages are incapable, as a matter of law, of having any modifying effect on the specific contract between the parties. (at [5])

Accordingly, the fact that a variation agreement has been reached by email or other electronic communications will not necessarily preclude a finding that the variation agreement is in 'writing'.

4.2.3 Signature

The analysis of whether or not an electronic variation agreement can be said to be 'signed' is similar to the discussions in section 3.12 (relating to statutory requirements for contracts to be signed).

While it appears that s 14 of the ETQA may potentially be relied upon to establish that an electronic variation agreement that has been authenticated by an electronic or digital signature has been 'signed', the main issues that may be encountered are:

- whether a contractual requirement for the variation to be signed can be said to constitute a signature requirement under a 'State law';

- whether consent has been given to the use of the signature method; and

- whether, having regard to all relevant circumstances at the time the signature method was used, the signature method was as reliable as was appropriate for the purposes for which the information was communicated.

As previously noted, until there are further judicial decisions on the application of s 14 of the ETQA, it is difficult to determine how a court will approach these issues.

Under the general law, there is authority to suggest that an electronic signature will constitute a sufficient signing of a variation agreement (for example, refer to the above discussions on *Hall v Cognos Ltd* (Industrial Tribunal Case No. 1803325/97) and the various cases referred to in section 3.12 above). However, the position with respect to digital signatures remains unclear.

Accordingly, the fact that a variation agreement has been reached by email or other electronic communications will not necessarily preclude a finding that the variation agreement has been 'signed'.

4.2.4 Conclusion

Until the courts have had the opportunity to consider the various provisions of the ETQA, it is difficult to conclude whether the ETQA may be relied upon to establish that an electronic agreement to vary a construction contract will constitute an agreement that is in 'writing' and 'signed'. However, under the general law, there is authority to suggest that an electronic agreement that has been authenticated by an electronic signature (or potentially a digital signature) will amount to an effective variation of the construction contract as it is in writing and signed.

Given the uncertainty on these issues, it will be vital for contracting parties to expressly address the issue of electronic communications in their contract documents. The risk for contracting parties is that 'email traffick' passing between them may give rise to an effective variation of the contract. This risk is increased where parties engage in regular email or other electronic communications in the day to day administration of their contracts, as this could amount to consent under the relevant provisions of the ETQA.

For parties who do wish to be bound by their electronic communications, it will also be important to include appropriate provisions in the contract setting out the status of electronic communications. However, as discussed further in the section below, careful consideration must be given to any such provisions as there may be particular types of communications under the contract (for example, variations to the contract and notices of default) which the parties still prefer to take place in paper form (Briggs & Brumpton 2001, p30).

4.3 Electronic notices

Building and construction contracts invariably contain contractual provisions that govern the delivery of various notices and certificates under the contract. Whether such notices may be validly delivered by an electronic communication will, for the most part, depend upon the terms and conditions of the relevant construction contract.

If the contract is absolutely silent as to communications under the contract, it is possible that the ETQA and general law contractual principles may recognise the validity of a notice that has been delivered by electronic means. However, where the contract contains a specific notice provision but such provision does not refer to electronic communications, it may be unlikely that a court would uphold an electronic notice as being valid. Ultimately, the issue would be resolved by interpreting the notice provision contained in the contract. As far as the ETQA is concerned, one of the main issues that would need to be considered is whether from the conduct of the parties and the surrounding circumstances, the parties have impliedly consented to notices being given by electronic communications (Mallesons 2003).

It will be imperative for construction contracts to include appropriately drafted notice provisions that clearly identify the parties' intentions as to whether notices may be validly delivered by electronic communications. It has been suggested that if the parties specifically allow for electronic notices in their contract, then it is likely that the courts will interpret this strictly and hold the parties to their intention (Mallesons 2003). An example of this approach may be found in the Canadian decision in *Kanitz v Rogers Cable Inc* (2002) 21 BLR (3d) 104, where a court held that the plaintiffs were obliged to continually inspect the defendant's website for updates to a user agreement, as the user agreement made specific provision for this to occur (Mallesons 2003).

In light of the importance of contractual notices (and depending on the circumstances of the parties and the security of their communication systems), it has been suggested that as a general rule, email should not be used for the delivery of contractual notices, as opposed to day-to-day correspondence (Mallesons 2003). If the parties wish to contractually avail themselves of effective electronic communications for some, but not all contractual notices, any notices that are intended to remain paper based should be clearly excluded by appropriate contractual provisions (Briggs & Brumpton 2001, p30).

Accordingly, regardless of whether or not the parties to a construction contract wish to be bound by electronic communications, the only way to clarify the legal uncertainties about the validity of electronic notices is to incorporate clear provisions within the construction contract.

4.3.1 Conclusion

If a construction contract does not contain a specific provision for notices to be sent electronically, depending on the conduct of the parties and the surrounding circumstances, it is still possible that the ETQA and the general law may recognise the validity of an electronic notice. To avoid the legal uncertainties about the status of electronic notices, construction contracts should contain clear provisions setting out the parties' agreement as to how valid notices may be given under the contract.

4.4 Protocols

To ensure that all participants in an electronic contract are able to communicate without misunderstanding, an agreement should be made as to the format of the data exchanged between the participants. It is recommended that an XML (eXtensible Markup Language) format be used to format data to be exchanged in an electronic contract. XML is a text based format based on tags similar to the well-known HTML format used to represent web pages.

XML has several advantages over other formats. Data stored in XML format uses tags to provide meaning to information which is not always the case for other data formats. Data is stored in text so that it is human readable and also machine readable. It is expected that participants in an electronic contract will view contracts using a collaboration tool or other application. If a particular XML format is agreed upon this means that different tools should be able to interpret and display the data in the same way that different web browsers can display the same web page.

XML is a very generic format. A commonly agreed set of tags needs to be defined for a particular context. This set of tags is commonly known as an XML schema. XML schemas exist for a large number of different topics and areas of interest that need to have formatted data. In particular, XML is heavily used as a format for document storage and processing both online and offline. The XML schema that would most likely be of interest for electronic contracting is the ebXML (Electronic Business (eBusiness) eXtensible Markup Language) schema that has been developed by OASIS (Organisation for the Advancement of Structured Information Standards) and the United Nations/ECE agency CEFACT. ebXML is a set of specifications with the aim of enabling electronic trading relationships between business partners.

4.5 Online collaboration platforms

4.5.1 Introduction

The construction industry has begun to adopt online collaboration platforms as a means of administering construction contracts. An example of an online collaboration platform in use within the Australian construction industry is Optus inCITE (Taylor, 2005). An online collaboration platform is an electronic network linking different organisations for the purpose of exchanging information electronically. Documents are stored on an electronic database that contains all the information relevant to the particular project. The database can be accessed by any project participant at any time and from any place. Different organisations or individuals may have different levels of access to different documents within the database (Briggs & Brumpton 2001, p29). The database is generally maintained by an external service provider who will have a contractual arrangement with at least one of the participants in the project (Kamara & Pan 2004, p57). Wilkinson (2005, p7) defines 'construction collaboration technology' as:

> A combination of *technologies* that together create a single shared interface between multiple interested individuals *(people)*, enabling them to participate in creative *processes* in which they can openly share their collective skills, expertise, understanding and knowledge *(information)*, and thereby jointly deliver the best solution that meets their common goal(s), while simultaneously creating an auditable electronic record of the people, processes and information employed in the delivery of the solution(s).

The use of online collaboration platforms in construction projects can result in significant benefits to industry. Tuma and Ward (2000) have summarised the benefits of online collaboration platforms in the following way:

> Internet contracting enables faster time to market by eliminating delays caused by sequential project information flow and decision making. This is accomplished by providing instant access to the latest validated project information. It also enhances control by providing security down to the document level and by providing a permanent audit trail of document access and decision making throughout the project life-cycle. Cyber contracting also increases revenue by improving team productivity through streamlining administrative procedures, by eliminating non-value added work, and by simplifying approval processes and automating workflow. In addition, geographic barriers to collaboration are eliminated, creating an environment where all team members have the most current information at all times. Reductions in cost result by eliminating unnecessary printing, copying, and delivery of drawings, by facilitating real-time communications, and by controlling travel costs. It reduces risk and liability associated with projects by capturing an audit trail of the entire design and building activity, thereby lowering the likelihood of disputes during and after the project.

4.5.2 The issues associated with collaboration platforms

A review of the literature reveals the following issues in connection with the use of online collaboration platforms in the construction industry:

- Disruptions may occur if the service provider is unable to maintain the service due to either technical difficulties or the cessation of the service provider’s business.

- The contractual arrangements between the service provider and the customer, and between the service provider and end users must be considered.

- Project protocols should be established setting out the standards for participants working on the project.

- The ownership of drawings and other documents and data stored in the database must be addressed and steps put in place to ensure that intellectual property infringements do not occur.

- The database should be maintained in such a way as to ensure the admissibility of the electronic records as evidence. An issue which will arise is that the system should track changes to documents so that the identity of the person making the change and the time of the change can be proven.

- Procedures should be agreed for archiving the database at the completion of the project.

- The system must have adequate security to ensure that unauthorised persons do not have access to the database and different participants should have different levels of access to the database depending on their role in the project.

- It may be difficult to ensure that all participants in the project use the collaboration platform rather than alternative means of communication such as email.

4.5.3 Disruptions to service

An efficient online collaboration can require 24 hour access for users who may be situated in different time zones. Accordingly network availability will clearly be an issue. The agreement with the service provider should contain provisions regarding times when the system may be unavailable to users and the notification that is required to be given to users in the event of unscheduled down time. The agreement should also be clear as to what will happen if the project extranet crashes (Wilkinson 2005, p115).

Project participants should consider whether their interruption to business insurance policy covers them for liability in the event that they suffer loss as a result of the collaboration platform being unavailable (Berning & Diveley-Coyne 2000).

It is also possible that a service provider will become insolvent. The agreement between the service provider and the customer should include provisions that apply in the event of the service provider's insolvency. These may include a right to transfer the contract to an alternative service provider (Wilkinson 2005, p117).

4.5.4 Contractual arrangements

4.5.4.1 Agreement between the service provider and customer

The agreement between the service provider and the customer should include provisions relating to the following matters (Wilkinson 2005, p111):

- The grant of a licence to the customer to access and use the collaboration service in relation to the project.
- Restrictions on the use of the collaboration system for unlawful purposes.
- The parameters governing the use of project data by the service provider and the project participants.
- The terms of the end-user licence agreements that will be entered into between the service provider and the other project participants.
- Payment terms.
- Ownership of copyright in the collaboration platform technology.
- The service provider's use of the customer's branding and data.
- Indemnification of the service provider against unauthorised use of the collaboration platform.
- Confidentiality, including the security of user names and passwords.
- The termination of the project including storage of data when the project is complete.
- Jurisdiction and choice of law.
- Any limitations upon the service provider's liabilities.
- The levels of service to be provided by the service provider including specifications as to security, backup systems, integrity of data, audit trails, access controls, technical specifications, system availability, software upgrades, customer support and end-user training.

4.5.4.2 End user licence agreement

Ideally, the agreements entered into between the service provider and the various project participants should be identical and there is a strong argument that such an agreement should be annexed to contracts appointing any consultants who will use the collaboration platform (Wilkinson 2005, p111). The end user licence agreements should include provisions similar to those contained in the agreement between the service provider and the customer and in particular, provisions relating to (Wilkinson 2005, p116):

- The project participant’s licence to access and use the collaboration platform.

- Circumstances in which the participant’s licence might be terminated (e.g. if they are no longer a participant in the construction project).

- The grant of a licence to the service provider to store and access any documents in which the project participant owns the intellectual property.

4.5.4.3 Agreement between project participants

The contract between the head contractor and any sub-contractors who will use the collaboration platform should also contain specific provisions to take into account the electronic management of the construction project.

Where a shared database is used for the storage of documents such as plans, there will be a greater possibility for there to be intellectual property infringements. As a consequence, the contract should deal with issues of design copyright, database ownership, confidentiality and commercial advantage (Briggs and Brumpton 2001, pp30-1). Intellectual property issues are discussed in ore detail in section 4.5.6 of this Report.

The contract should also include a provision that electronic records that comply with specified archiving and authentication procedures are deemed to be admissible as evidence and prima facie accurate (Reed 2001, p91).

4.5.5 Project protocols

The service provider should establish a project protocol document setting out the rules of operation for project participants working on the collaboration platform. Wilkinson (2005, pp114-15) identifies the following requirements of the project protocol document:

> Typically, it will:
>
> - provide common protocols describing how users publish, retrieve and manage information quickly and efficiently;
> - establish security levels, including access rights for different team members and different types of information;
> - be modified by the client and/or the project team to suit its processes;
> - as a ‘live’ document, be maintained and updated as required by the client/team;
> - need to be read in conjunction with non-project-specific guides on use of the collaboration system (e.g.: user guides, etc.);
> - detail the pragmatic working procedures to be followed by participants during any temporary suspension of service (such procedures are essential to ensure the integrity of the data once the service recommences).

4.5.6 The ownership of documents and intellectual property

Architects and designers may be concerned that their intellectual property rights in drawings are more likely to be infringed where they are submitted in their original electronic format and stored on the collaboration platform. Practical means of protecting copyright in drawings are to (Wilkinson 2005, p121):

- Include a disclaimer and statement of permitted use of all drawings;

- Include the architect’s name and logo and copyright statement on all drawings; and

- Watermark the drawings with the architect’s name or logo.

Contracts should also include explicit confidentiality and copyright licensing provisions. Contracts with designers usually provide that the designer retains copyright in the design and grants a licence to the client and other project participants to use the design in relation to the project (Wilkinson 2005, p121). Even if the contract does not contain such a licence, there would be an implied licence to use the plans for the purposes of the project (*Gruzman Pty Ltd v Percy Marks Pty Ltd* (1989) 16 IPR 87). The use of a collaboration platform would not normally change the legal position with regard to the ownership of designs. Wilkinson (2005, p121) notes, however, that it is possible that if designs are amended extensively by online collaboration it may be that the authorship of the design can no longer be said to rest with the original designer. Contracts should include provisions to deal with this possibility.

4.5.7 Archiving

Upon completion of the construction project the database may continue as an online facility which continues to be able to be updated. In this case the software would also continue to be updated so that the customer need not be concerned with the continued readability and availability of the data (Wilkinson 2005, p122). Alternatively, the data can be stored in an off-line archive. In this case it may also be possible to produce a copy of the project for project participants on CD ROM or DVD (Wilkinson 2005, p122). The parties should agree contractually before the project begins, how the project data will be archived and what data will remain available to each project participant (Berning & Diveley-Coyne 2000).

In choosing a method of archiving the project database the issues raised in section 5.6 of this Report should be taken into consideration.

4.5.8 Evidentiary considerations and audit trails

The evidentiary considerations that arise generally in relation to electronic records are considered in sections 5.2 and 5.3 of this Report. Particular issues in relation to collaboration platforms are:

- The service provider should ensure that a rigorous audit trail is kept logging the time of creation of a document, by whom it was created, when it is sent and received and when and by whom changes to the document are made (Wilkinson 2005, p119).

- The collaboration platform must ensure that the integrity of the electronic records can be proven so that a court can be satisfied that an electronic record produced in court is unaltered from the original document. Compliance with recognised codes of practice and standards dealing with electronic record keeping would assist in satisfying the court that the integrity of the electronic records has been maintained (Wilkinson 2005, p110).

- Where a collaboration platform is used, the cost and time involved in the document discovery process in the event of a dispute can be significantly reduced (Wilkinson 2005, p119). This is because a complete record of the construction project is maintained by the collaboration platform rather than documents being stored in various formats (paper and electronic) and in various locations. This advantage will be lost if participants in the project also use alternative means of communication and document storage such as private email and paper documents.

4.5.9 Access controls

To alleviate concerns about the security of data, web collaboration platforms should be designed so that parties have limited access to data, depending on their role within the project. Berning and Diveley-Coyne (2000) note:

> For example, a subcontractor may only have access to drawings and communications relating to its part of a project while other information may be shared with all parties involved. A general contractor may use the Web site to perform budget analysis and communicate with its employees regarding costs, information that it may not want the owner or subcontractors to access. Accordingly, project Web sites must have a strong security system to limit access and prevent breaches.

The rights to view and alter data are controlled by an access control system. The components of an access control system are:

- the identification of the user by him or herself;
- the authentication of the identity of the user by the system; and
- the authorisation of the user to either view or alter data by granting specific rights.

4.5.9.1 Identification

The identification stage of the process is the method by which a user tells the system who he or she is (for example, by using a username). Identification is usually based on parameters such as:

- the name of the computer;
- the physical address of the computer or Media Access Control address;
- an Internet Protocol address; and
- the process identifier (or process ID) which is a number used to uniquely identify a process.

The identification component of an access control system should meet the following requirements:

- it must uniquely identify the user;
- it should not identify the position of the user or the user's relative importance in the organisation; and
- it should avoid using common or shared user accounts, such as root, admin and sysadmin. Such accounts provide no accountability and are targets for hackers.

4.5.9.2 Authentication

Authentication is the process of verifying the identity of the user. Examples of authentication processes include comparing an entered password to the password stored on a system for a given username and comparing the hash code of an entered password to the hash code of the password stored in the computer. Authentication relies on one or more of the following factors (NOIE 2002):

- Something the user knows, such as a password or a personal identification number (PIN). This assumes that only the owner of the account knows the password or PIN needed to access the account.
- Something the user has, such as a smart card or token. This assumes that only the owner of the account has the necessary smart card or token needed to unlock the account.
- Something the user is, such as fingerprints or the voice, retina or iris characteristics of the user (biometrics).

The most secure methods of authentication involve a combination of two or more of the above factors (e.g. the use of a security token that generates a one time password). The more secure methods of authentication are more expensive and a cost-benefit analysis is necessary to determine the level of authentication required. In the context of electronic contract administration a password based authentication system may provide a sufficient level of authentication.

4.5.9.3 Authorisation

Authorisation refers to the rights of a user to access and alter data on a system. The rights that may be granted to the user are:

- Read: The user can:
    - Read file contents; and
    - List directory contents

- Write: The user can change the contents of a file or directory with these tasks:
    - Add;
    - Create;
    - Delete; and
    - Rename

- Execute: If the file is a program, the user can run the program.

These rights or permissions are implemented differently in systems based on discretionary access control, mandatory access control, role based access control and location based control policies. Discretionary access control systems allow the owner of the data to determine what access rights are granted to the data (Pfleeger 1997). For example, an organisation that initiates an e-contracting process (i.e. the owner of the e-contracting process), can authorise all or only some of their employees to participate in the contracting process.

In a mandatory access control system, a central authority or system determines the user's access rights and the user cannot change his or her access rights. For example, an organisation may allow a clerk to modify any contract initiated by the organisation or may limit the clerk to modifying only those contracts initiated by the clerk (Goodwin et al. 2002).

A role based access control system restricts access to authorised users based on the roles assigned to individual users (Ferraiolo & Kuhn 1992). Access control decisions are based on the functions or roles a user is allowed to perform within an organisation and, unlike a discretionary access control policy, users cannot pass access permissions onto other users at their own discretion.

A location based access control system is based on geography or location (Goodwin et al. 2002). For example, contract clerks who are located at the business headquarters might be able to modify any contract, whereas those located at a branch office may only able to modify the contracts initiated by them.

An alternative to the access control systems described above is the use of an application that employs Extensible Access Control Markup Language (XACML). Where organisations use browser-based access to portals that aggregate resources such as web pages, applications and services, the server must determine whether the client is authorised to use a particular resource.

XACML provides a policy language, which allows administrators to define the access control requirements for their application resources. XACML is a general purpose access control policy language. It provides syntax defined in XML for managing access to resources.

XACML is used whenever an organisation needs rules to control access to some resources. It may be imbedded in products such as gateways, firewalls, web servers, application servers or provided by a specialised access control product. XACML has two basic components. The first is that it provides a flexible language for expressing access control that can use virtually any sort of information as the basis for decisions. The second is a request/response language that presents requests for access and describes the answers to those requests.

The control of activities such as read, write, copy and delete provided by XACML depends on several criteria such as the attributes of the user requesting access (for example, only contract administrators and those above them in the organisation's hierarchy may alter the contracts), the protocol over which a request is made (for example, viewing data accessed only via HTTPS) and authentication mechanisms (for example, the requestor of the resource must be authenticated using both a password and a smart card).

4.5.10 Security

One of the most serious concerns that the construction industry has in relation to the use of collaboration platforms is the security of confidential information that is made available via the platform (Berning & Diveley-Coyne 2000). Issues in relation to the control of access to data by the various participants in the project have been discussed in section 4.5.9 of this Report. A further issue arises in keeping the data secure from unauthorised access whether by a party to the project or an outsider. A security policy determines who will have access to different types of data and whether or not they have a right to alter the data. The method by which the security policy is implemented is referred to as a security model (Gollmann 1999).

Security models address the confidentiality (Bell & LaPadula 1973, Bell & LaPadula 1975) and the integrity (Biba 1977, Clark & Wilson 1987) of data. The Bell-LaPadula model ensures confidentiality of classified information to which access is restricted to a particular class of people. A pure Bell-LaPadula model is not recommended for the implementation of security policies in the context of electronic contracting as it only ensures confidentiality of classified information and does not address integrity.

The Clark-Wilson model ensures the integrity of information in a commercial environment by attempting to prevent the unauthorised modification of data. The model emphasises the control of transaction processing. Data (e.g. a database) can be accessed only by a specific set of procedures (e.g. a defined search of the database). Users have access to the procedures but do not have access to data items, ensuring that any alteration of data complies with an organisation's integrity rules (e.g. each data item can be manipulated by a particular set of programs only). The model also maintains an audit log to track alterations to data (Shrivastava 2004).

The Brewer-Nash Chinese Wall Model is a confidentiality model that prevents conflicts of interest with respect to dealings by an organisation with different clients (Brewer & Nash 1989). Data is classified into datasets relating to different clients or transactions. Access to a dataset relating to one client will prevent access to the dataset relating to a different client or transaction.

It is recommended that in the context of electronic contracting, the Clark-Wilson and Chinese Wall models be used one on top of the other. While the Clark-Wilson model ensures the integrity of data, the Chinese Wall model ensures confidentiality between different projects with which an organisation is involved.

4.5.11 Ensuring the use of collaboration platforms

While it is apparent that there are several advantages to industry in the use of collaboration platforms in construction contract administration, there is a strong resistance from industry participants to adopt these new technologies in their full capacity, and to change how work has traditionally been done in the industry (Becerik 2004, p1).

As noted in section 4.5.8 of this Report in relation to evidentiary considerations, if participants use alternative communication and storage methods then the discovery benefits that flow from the use of a collaboration platform will be lost. Accordingly, it is essential that project participants adopt clear policies in relation to the types of communications and documents for which the collaboration platform should be used and that staff members are encouraged to use the collaboration platform in accordance with those policies.

It may be possible to include a provision in agreements between the head contractor and subcontractors requiring that the collaboration platform be used for all communications between the parties (Wilkinson 2005, p111). However, as noted in section 4.3 above, any contractual notice provisions would need to be carefully drafted to ensure that they accurately reflect the parties' intentions on the use and validity of electronic communications.

4.5.12 Conclusion

It is clear from the discussions above that while the use of collaboration platforms has the potential to improve efficiency in the management of construction projects, various issues need to be carefully considered and addressed before a collaboration platform is implemented. These issues have resulted in a delayed take up of available technology by industry (Wilkinson 2005, p107).

The following issues have been revealed by the literature in relation to collaboration platforms:

- **Practical issues:** Practical issues of concern include the potential disruption to the availability of the platform due to either technical difficulties or cessation of the service provider's business, and difficulties in ensuring that all participants in the project use the collaboration platform rather than alternative methods of communication (e.g. email).

- **Legal issues:** Potential legal issues include the contractual arrangements that must be put into place between the service provider and the customer and between the service provider and end users; intellectual property issues that may arise out of the storage of drawings and other documents and data in the database; evidentiary issues arising out the creation and storage of electronic documents and the requirement to archive the database in order to comply with legal requirements.

- **Technical issues:** Technical issues include establishing project protocols setting out the standards for participants working on the project, the security of confidential information and the control of access to information by the various participants in the project.

Potential users of collaboration platforms must ensure that they obtain appropriate legal and technical advice before making a commitment to use a platform for a construction project. In addition appropriate policies should put in place to ensure the collaboration platform is used within the organisation in the intended way.

5. ELECTRONIC RECORDS MANAGEMENT

5.1 Overview of issues associated with electronic records management

A review of the literature, judicial decisions of the courts and legislation reveals that the legal considerations arising from the use of electronic communications and records in the management of construction projects are:

- The effective management of construction projects necessarily entails a range of communications passing between a large number of project participants. Where these communications occur electronically, a number of complex legal issues arise about whether or not the electronic communications may be used as evidence and the evidential weight that may be attributed to them. A summary of the legal position in relation to electronic documents that may be commonly used in the construction industry is produced below. (Refer to section 5.4)

- There is legal uncertainty as to whether electronic records relevant to a construction project can be relied upon as evidence in court. (Refer to section 5.2)

- It is uncertain whether electronic records will be given the same weight in court as their paper based equivalents. (Refer to section 5.3)

- Electronic records must be carefully managed to ensure that construction project participants are in a position to comply with their discovery obligations in the event of litigation. (Refer to section 5.4)

- Construction project participants must preserve electronic records in a way that satisfies all legal requirements governing the retention of records. (Refer to section 5.5)

‘Electronic records’ refers to any records generated by, or stored on, a computer system. Electronic records fall into three categories. First, they may be created by humans but are stored electronically (e.g. emails). Secondly, they may be computer generated records such as log files, telephone records or ATM transaction receipts. Thirdly, they may be a combination of computer stored and computer generated, such as information contained in financial spreadsheets (Standards Australia 2003, pp2-3).

Casamassima and Caplicki (2003, p13) note that various electronic records are created and stored by organisations that are involved in construction projects:

> These electronic records include financial data, such as general ledgers, job costs, material invoices, and labour records; the baseline CPM schedule and the periodical updates to the schedule; daily reports of supervisors and foremen; change orders; requests for information; meeting minutes; and all sorts of records necessary to the progress of the construction project.

Different evidentiary considerations will apply depending what type of electronic record is under consideration.

5.2 Admissibility of evidence

5.2.1 Sources of the rules of evidence in Australia

The rules of evidence in Australia arise from the common law and from Commonwealth, State and Territory legislation. Different rules may apply depending on the court in which litigation takes place. Proceedings in Federal courts are governed by the *Evidence Act 1995*

(Cth) and the applicable rules of court, whereas proceedings in State courts will be governed by the relevant State Evidence Act and the applicable rules of court.

The *Evidence Act 1995* (Cth) was intended to be the basis of a uniform legislative scheme throughout Australia. The *Evidence Act 1995* (NSW) and the *Evidence Act 2001* (Tas) mirror the Commonwealth Act, although there are some differences (ALRC 2005, p29), and the Commonwealth Act applies by agreement in the Australian Capital Territory. The Acts based on the Commonwealth Act are known as the **uniform Evidence Acts**.

In summary, the uniform Evidence Acts apply to all proceedings in Federal courts, or courts of the Australian Capital Territory, New South Wales and Tasmania. Proceedings in Queensland Courts are governed by the *Evidence Act 1977* (Qld). Proceedings in other State courts are governed by the relevant State Evidence Act.

5.2.2 What is evidence?

The facts in dispute in any court proceeding are proved by admissible evidence. Evidence may be:

- **Testimony** - Testimony is the oral evidence given by a witness. Oral evidence is given by a witness who has personal knowledge of the facts. It is considered reliable because the witness has sworn an oath and been exposed to cross-examination.

- **Documentary evidence** - The precise definition of documentary evidence will vary depending on the context in which it is used. A broad definition would include all records of information made by processes whereby information is stored and can be retrieved (Ligertwood 2004, p457).

- **Real evidence** - Ligertwood (2004, p467) defines real evidence as 'information experienced directly by the trier of fact and not reported through the testimony of a witness.' Examples of real evidence include objects such as murder weapons, a viewing of a relevant location and recordings such as photographs and tape recordings.

To be admissible the evidence must (Laryea 1999, para 8):

- be relevant either to proof of a fact in dispute, to the credibility of a witness or to the reliability of other evidence; and

- not be inadmissible by reason of some particular rule of law such as the rule against hearsay.

Evidence will be relevant if it tends to prove one or more of the facts in issue in the dispute. Relevance is of no greater issue in relation to electronic records than it is in relation to other types of evidence (Laryea 1999, para 9). Once it is found that particular evidence is admissible, it will be for the court to determine the weight to be attached to the evidence, i.e. whether or not to believe or act on the evidence.

The types of evidence that will be relevant to construction project litigation will include the construction contract, communications between project participants (including email communications), notices and variations made under the contract, project records generated during the normal course of construction and financial records.

5.2.3 The international position

Article 9 of the UNCITRAL Model Law on Electronic Commerce 1996 provides:

> (1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

> (a) On the sole ground that it is a data message; or
>
> (b) If it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in it original form.
>
> (2) Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

The two essential elements of Article 9 are that a data message should not be denied admissibility on the sole ground that it is a data message and that the data message should be afforded due weight as evidence (ECEG 1998, para 2.9.13). Article 9 has not been implemented in Australia. The Electronic Commerce Expert Group, which considered the implementation of the UNICTRAL Model Law on Electronic Commerce 1996, was of the view that the admissibility and weight of electronic records should be dealt with by the Commonwealth and State Evidence Acts (ECEG 1998, para 2.9.14). Accordingly, there is no specific provision applying uniformly in courts throughout Australia addressing the issues of admissibility and weight of electronic records as evidence.

5.2.4 Hearsay rule

Definition of the hearsay rule

The hearsay rule applies to statements made outside of court by humans. It does not operate to exclude documents unless they are being relied upon to prove the truth of a statement made out of court. Therefore the rule will not apply to prevent an electronic contract from being admitted to establish the terms of the contract.

Where electronic records are sought to be used as proof of the statements contained in them they may be inadmissible due to the hearsay rule. The hearsay rule makes inadmissible any statements made out of court which are tendered in court for the purpose of directly proving the facts asserted in the statement (*Walton v The Queen* (1989) 166 CLR 283, 288).

The hearsay rule extends to statements made in written documents (*Myers v DPP* [1965] AC 1001) so that if a document is used as proof of the facts asserted in it, then it will be inadmissible hearsay (Forbes 2004, p300). For example, if an email contains an observation by the author about the state of progress of a construction project, the hearsay rule would render the email inadmissible as proof that the project was at that stage.

If an electronic record is sought to be admitted not as evidence of the truth of the statement contained in the record but for some other reason (such as proof that the statement was made), the hearsay rule will not prevent its admissibility. For example, the hearsay rule will not be an objection to the use of electronic evidence for a purpose such as showing that notice has been given pursuant to the contract or establishing what are the terms of a contract (Cassamassima & Caplicki 2003, p17). Accordingly, where a contract is formed electronically the electronic contract will not be inadmissible due to the hearsay rule. The evidentiary issue with regard to an electronic contract or notice will be establishing the authenticity of the document.

Construction litigation relies heavily upon the use of project records which contain statements by humans. Accordingly, the hearsay rule will be regularly encountered during construction litigation (Casamassima & Caplicki 2003, p13). Where electronic records are the result of human involvement (such as emails and other computer stored records) they may be found to be inadmissible as evidence because of the application of the hearsay rule. In that case in order for the electronic records to be admissible as evidence, it will be necessary for them to fall within one of the exceptions to the hearsay rule.

If the electronic records are computer generated records made without human involvement (such as computer traces of log on records) they may be admissible as real evidence and the hearsay rule will not apply. This is because the hearsay rule is only directed to ensuring that the evidence of humans is given by way of oral testimony that is given under oath and that can be tested in court by cross-examination.

Whether the electronic record is treated as documentary evidence (to which the hearsay rule applies) or real evidence (to which the hearsay rule will not apply) it will be necessary for the evidence to be authenticated by evidence that the computer system that generated the record was functioning correctly at the time the record was generated.

Application of the hearsay rule

In Queensland the hearsay rule continues to apply by virtue of the common law. While the Queensland Act has created various exceptions to the rule, the common law exceptions have not been excluded and continue to apply. Under the uniform Evidence Acts, the hearsay rule applies by virtue of s 59. There are various statutory exceptions to the hearsay rule under the uniform Evidence Acts and the common law exceptions generally no longer apply. However where the hearsay rule did not apply at common law (for example because the document produced did not contain a statement by a human) the exclusionary rule will continue to apply under the uniform Evidence Acts. It is therefore important to discuss the common law exceptions to the hearsay rule.

5.2.4.1 Common law exceptions

The common law rules of evidence include numerous exceptions to the rule against hearsay, two of which are of particular relevance to electronic evidence. The hearsay rule will not apply to output that is generated by a computer acting as a scientific instrument and it will not apply to data independently recorded by a computer without human involvement.

Computer acting as a scientific instrument

Firstly, the hearsay rule does not apply to output that is generated by the computer acting as a calculator or scientific instrument i.e. where the output is generated automatically by the computer following previously programmed instructions without further human intervention (Halsbury, para 195-4005; *Mehesz v Redman (No 2)* (1980) 26 SASR 244; *R v Weatherall* (1981) 27 SASR 238 at 247; *R v Wood* (1982) 76 Cr App R 23; Forbes 2004, 338).

In *R v Wood* (1982) 76 Cr App R 23, it was held that computer analysis of various metals would be admissible as real evidence because the computer was acting as a scientific instrument. The fact that the computer process involved humans in order to program it to perform the calculation did not mean that the hearsay rule applied. In *Mehesz v Redman (No 2)* (1980) 26 SASR 244 it was held that the results produced by a breath analysis machine were admissible as real evidence.

In *Rook v Maynard* (1993) 2 Tas R 97 printouts of computer traces of log-on records were held to be prima facie admissible as the trace program was entirely mechanical. In this type of situation the hearsay rule does not apply because the evidence produced is created by a machine and is not the testimony of a human.

Computer recorded data

Secondly, the hearsay rule does not apply to data independently recorded by a computer without significant human involvement, such as data captured by a surveillance camera or breathalyser (*Castle v Cross* [1984] 1 WLR 1372; Forbes 2004, p337).

In *Sapparo Maru v Statue of Liberty* [1968] 2 All ER 195 the record made by a radar of the sonar echoes of two ships involved in a collision was admissible. The evidence was found to be real evidence because it was made without human intervention and therefore the hearsay rule did not apply.

In *Inspector Stephen Campbell v James Gordon Hitchcock* [2003] NSWIR Comm 148 the NSW Industrial Relations Commission found that a database maintained by the New South Wales Safe-T-Cam system which involved monitoring of heavy vehicle movements by digital camera technology did not involve any representation by a person and therefore did not attract the application of the hearsay rule.

Computer stored vs computer generated records

As a result of these two common law exceptions the hearsay rule would not apply to exclude computer generated electronic records. However, where the electronic record is a computer stored record rather than a computer generated one, the hearsay rule will be relevant. This is because computer stored records are generated by humans and are therefore statements made out of court. Examples of computer stored records include word processed files, spreadsheets, charts, graphs and emails. Examples of computer generated records are trace reports created by telephone companies, ATM receipts, meta-data and internet protocol logs (Wolfson 2005, pp157-9). Computer stored records will only be admissible if one of the exceptions to the hearsay rule applies (Halsbury 1991, para 95-4010).

Proof of accurate working of computer

Where computer generated electronic records are sought to be admitted there generally must be testimony that the records are correct. Where a scientific instrument is well known there is a presumption that it is trustworthy so that a reading from such an instrument is prima facie evidence of the facts recorded without a requirement to test the instrument’s accuracy. Where the instrument has not yet become so well known that its accurate working can be presumed, there must be evidence given to establish that the scientific instrument is one which is likely to produce accurate results (*Porter v Kolodzeij* [1962] VR 78). This presumption will not apply to the workings of machines that are not well known and may not apply to computer programs.

In *Chio Yaou Fa v Morris* (1986) 46 NTR 1 the court held that a satellite navigation system was not so well known that it would be presumed to be trustworthy. The court would not presume new instruments to be trustworthy until they had gained sufficient recognition that judicial notice could be taken of their trustworthiness. Until that happened, the accurate working of the instrument must be proven before the evidence will be accepted. In that case insufficient evidence had been given of the accuracy of the satellite navigator and therefore the evidence was inadmissible.

The accurate working of a computer program may be proven by (Halsbury 1991, para 195-4015):

- Evidence given by the programmer;
- Evidence given by the operator of the computer program (*R v McHardie* [1983] 2 NSWLR 733);
- Other evidence that the computer was competently maintained and that any malfunction has not affected the material produced by it (*Murphy v Lew* [1998] VR 791).

Summary of common law exceptions

In summary, the result of the common law exceptions to the hearsay rule is that documents that are computer generated and that do not contain any statements by humans will be admissible as real evidence. The types of documents that may be admissible under the exceptions include audit logs of computer systems, computer operated security cameras and documents produced by scientific measuring instruments.

5.2.4.2 Statutory exceptions

Queensland position

Summary of statutory exceptions in Queensland

The main provisions of the *Evidence Act 1977* (Qld) that allow statements in documents to be admissible in civil proceedings as an exception to the hearsay rule that will be relevant in a construction context are:

- Section 84 – books of account.
- Section 92 – admissibility of documentary evidence in civil proceedings (the 'business records exemption').
- Section 95 – statements produced by computers.

'Document' is defined in s 3 to include books, maps, plans, drawings and photographs, and any disk, tape, recorded track or other device in which sounds or other data (not being visual images) are embodied so as to be capable of reproduction and any film, negative, tape or other device in which one or more visual images are embodied so as to be capable of reproduction.

Books of account

Section 84 provides that an entry in a book of account shall be evidence of the matters, transactions and accounts recorded. An electronic record such as a general ledger, invoice or labour record may be admissible as an entry in a book of account.

Business records

Section 92 contains two separate grounds for admissibility of statements in documents:

- where the maker of the statement has personal knowledge of the matters; and
- where the document forms part of a record relating to an undertaking and was made in the course of that undertaking from information supplied by a person who had, or may reasonably be supposed to have had, personal knowledge of the matters.

In both cases, the person who had the personal knowledge is ordinarily required to be called as a witness in the proceeding. However the maker of the statement is not required to be called if:

- they are dead;
- they are out of State and their attendance is not reasonably practicable;
- they cannot be found;
- they have no recollection due to the elapsing of time;
- they would not be permitted to be cross-examined; or
- undue expense or delay would be caused by their being called as a witness.

The types of documents that may be admissible under the business records exemption include:

- Balance sheets (*Valoutin Pty Ltd v Furst* (1998) 154 ALR 119);

- Valuation reports (*Ringrow Pty Ltd v BP Australia Ltd* [2003] FCA 933);

- Correspondence (*Freiberg International Pty Ltd v Iken Commercial Interiors Pty Ltd* [1995] ACTSC 42);

- Proofs of debt (*Rickard Constructions Pty Ltd v Rickard Hails Moretti Pty Ltd* [2004] NSWSC 984);

- Emails (*Rickard Constructions Pty Ltd v Rickard Hails Moretti Pty Ltd* [2004] NSWSC 984); and

- Computer stored records of golf scores kept by a golf club (*Cooper v Bankstown-Lidcombe Health Service (Lidcombe Hospital)* [1998] NSWCC 30).

In a construction project most project records will be categorised as business records and accordingly they may be admissible under s92.

The business records exemption can be applied to an electronic record provided the conditions of the section are satisfied. However, Laryea (1999, para 33) argues that the business records exemption under the Queensland Act is not ideal in ensuring free admissibility of computer data. Computer records are relegated to secondary status because they are only admissible if the supplier of the information is unavailable to testify.

Computer produced documents

Section 95 provides an exception to the hearsay rule for statements contained in documents produced by computers where:

- the statement is produced during regular use of the computer;

- data was regularly supplied to the computer in the ordinary course;

- there has been an absence of computer malfunction; and

- the statement reproduces information supplied to the computer in the ordinary course.

Compliance with these conditions may be proved by a certificate under s 95(4).

Section 95(7) defines ‘computer’ as ‘any device for storing or processing information’. Section 95 applies whenever computer information is sought to be admitted even if it would not be hearsay because it is computer generated (Halsbury, para 195-4035). However s95 does not apply if the evidence is admissible under one of the other statutory exceptions such as books of account or business records.

There is no requirement under s 95 that a person give evidence other than if required to satisfy the four conditions relating to the proper operation of the computer system.

Laryea (1999, para 27) argues that one would expect that computer evidence would be admitted under s95 with relative ease, however, notes that in the three cases heard prior to 1999 under the equivalent South Australian provision, the conditions of s95 were found not to have been met. In *Steiner v Modbury Towing Services* [1998] SASC 6774 computer records were held to be inadmissible because the party seeking to rely on the evidence did not prove that the computer was correctly programmed and regularly used to produce output of the same kind.

Reynolds (1994) argues that s 95 (and its equivalent in South Australia and the United Kingdom) is intended to apply to situations in which computers process information which results in new information rather than where the computer acts as a storage device for existing documents. Accordingly, documents such as emails would not be exempted under s 95 as they are not documents 'produced by computers'. This view does not appear to have been adopted in any of the judicial consideration of the equivalent statutory provisions. In *Mehesz v Redman* (1980) 26 SASR 245 at p254 White J said, in the course of considering the admissibility of evidence generated by a breath analysis machine, that the South Australian equivalent provision may well apply 'to the storage and retrieval type of computer and not to this kind of measuring computer.' Accordingly, the better view would appear to be that s 95 applies to computer stored documents as well as computer generated documents.

Conclusion: statutory exceptions in Queensland

The statutory exceptions under the Queensland legislation overlap, making the scheme a complex one (Forbes 2004, para 83.4). If an electronic record fails to be admitted under s 95 as a computer produced document it may still be admissible as either a book of account or a business record under ss 84 or 92 respectively. In that case it will not need to satisfy the four requirements of s 95.

Uniform Evidence Acts position

Summary of hearsay and statutory exceptions under the uniform Evidence Acts

Section 59 of the uniform Evidence Acts provides a general rule against hearsay:

> (1) Evidence of a previous representation made by a person is not admissible to prove the existence of a fact that the person intended to assert by the representation.

The uniform Evidence Acts provide numerous exceptions to the rule against hearsay. The exceptions that are relevant to the production of computer generated evidence are business records (s 69) and electronic communications (s 71).

Business records

Section 69 includes an exemption from the hearsay rule for business records. The section provides:

> (2) The hearsay rule does not apply to the document (so far as it contains the representation) if the representation was made:
> (a) By a person who had or might reasonably be supposed to have had personal knowledge of the asserted fact; or
> (b) On the basis of information directly or indirectly supplied by a person who had or might reasonably be supposed to have had personal knowledge of the asserted fact.
>
> (3) Subsection (2) does not apply if the representation:
> (a) was prepared or obtained for the purpose of conducting, or for or in contemplation of or in connection with, an Australian or overseas proceeding; or
> (b) was made in connection with an investigation relating or leading to a criminal proceeding.

'Document' is defined in the dictionary to the uniform Evidence Acts as any record of information including anything on which there is writing, marks or figures which can be interpreted and images or writings which can be reproduced with the aid of anything else. The Australian Law Reform Commission considers the definition to include computer storage methods such as disks and computer tapes (ALRC 1995, p285).

Unlike the equivalent provision in s 92 of the Queensland Act, there is no requirement that the maker of the statement give evidence.

In *Rickard Constructions Pty Ltd v Rickard Hails Moretti Pty Ltd* [2004] NSWSC 984 an email setting out costs claims for the purposes of quantifying damages resulting from a pavement failure was found to meet the requirements of s 69(2), however, the email was ultimately held to be inadmissible under s 69(3) on the basis that it was prepared in contemplation of legal proceedings.

In *Roads and Traffic Authority of New South Wales v Tetley* [2004] NSWSC 925 a 'Journey Report' which was described as a computer generated print-out derived from a Global Positioning System/vehicle monitoring information system was not admissible under s 69 as it did not contain any representation made by a person. It should be queried whether the Journey Report should have been admissible as real evidence on the basis that it did not involve human input.

The person who has the knowledge of the asserted fact need not have any particular relationship to the business whose record is sought to be admitted (*Penrith City Council v Penrith Waste Services Pty Limited* [1995] NSWLEC 176).

It should be noted that the exemption in s 69 does not apply to the whole document but only to the representations in the documents that qualify for exemption as either being made by a person who had personal knowledge of the asserted fact, or made on the basis of information directly or indirectly supplied by a person reasonably supposed to have had personal knowledge.

Representation in electronic communications

Section 71 of the uniform Evidence Acts provides that:

> The hearsay rule does not apply to a representation contained in a document recording a message that has been transmitted by electronic mail or by a fax, telegram, lettergram or telex so far as the representation is a representation as to:
>
> (a) the identity of the person from whom or on whose behalf the message was sent; or
>
> (b) the date on which or the time on which the message was sent; or
>
> (c) the message's destination or the identity of the person to whom the message was addressed.

Section 71 only applies to electronic mail, faxes, telegrams, lettergrams and telexes. Given the use of the narrow term 'electronic mail', which is likely to be restricted to email, the section may not apply to other forms of electronic communication such as electronic data interchange, internet relay chats, computer based instant messaging and phone text messaging (ALRC, 2005 pp150-155).

The s 71 exception relates only to the identity of the sender of the message, the date of the message and the destination of the message. It does not relate to the contents of the message.

5.2.5 Best evidence rule

5.2.5.1 Introduction

An issue may also arise as to whether electronic records are inadmissible as a result of the best evidence rule. The best evidence rule provides that where a document is tendered as evidence, the original document is required and a copy will not suffice. The best evidence rule has now been abrogated by the operation of Statute. However, where it does apply the issues raised in relation to electronic records are whether it is practicable to tender the original document in court, and which version of an electronic record is the original document.

At common law, the best evidence rule provided no evidence was admissible unless it was ‘the best that the nature of the case would allow.’ (*Ormychund v Barker* (1745) 26 ER 15, 33). As a result the contents of a document could only be proved by tendering the original document (ALRC 2005, p138). A copy would only be admissible if the original was unavailable and the copy was authenticated (Laryea 1999, para 44).

The issues posed by the best evidence rule in the digital environment are:

- What is the original record? In the case of email, is it the record stored on the sender’s or the receiver’s computer? The copy stored on the recipient’s computer may well include additional information such as the time of dispatch and receipt.

- Is it practicable to produce the original electronic record in court?

It may be unnecessary to determine these issues as the best evidence rule appears to have been abrogated by statute (Laryea 1999, para 48) and the common law. In *Butera v Director of Public Prosecutions for the State of Victoria* (1987) 164 CLR 180, 186 the High Court held that the best evidence rule should not apply to exclude copies of audio tapes ‘provided the provenance of the original tape, the accuracy of the copying process and the provenance of the copy tape are satisfactorily proved.’ By analogy, copies of electronic records should not be excluded provided that their integrity and authentication can be proved.

However even where the best evidence rule has been abolished or abrogated by statute or the common law it is still necessary to prove that the copy of a message produced is an authentic copy. In practice such authentication has not been difficult with courts being prepared to accept the authenticity of an electronic record if oral evidence is given that the computer system was operating correctly at the time and no evidence to the contrary is adduced by the other party (Reed 2001, p90).

5.2.5.2 Queensland position

Section 95 of the *Evidence Act 1977* (Qld) allows statements contained in a document produced by a computer to be admitted and s 97 provides that a copy of the document may be produced and may be authenticated in such manner as the court may approve. However, the weight to be given to the evidence is for the court to determine.

The best evidence rule may still be an issue where a print out is sought to be admitted in evidence where there is an original electronic record. Laryea (1999, para 49) argues that the requirement to produce an original document has not raised problems in practice. It may be that this is because the parties have not argued that the best evidence rule should exclude the admissibility of a print out of an electronic record because it has been assumed that print outs are acceptable copies of electronic data. Davidson (1999, p29) argues that the position in Queensland in relation to the admissibility of print outs of electronic documents such as emails is unclear, and that electronic versions of such documents should be kept for evidentiary purposes.

In *Armstrong v Executive of the President* 810 F Supp (1993) the court found that the printed version of an email contained less information than the electronic version; namely the date of transmission and receipt, the list of recipients, and linkages between messages sent and replies. Following from this decision it may be argued that a print out of an electronic record is not an acceptable copy if the meta-data contained in the electronic record is not included in the print out.

5.2.5.3 Uniform Evidence Acts position

Abolition of best evidence rule

Section 51 of the uniform Evidence Acts abolished the common law rules relating to the means of proving the contents of documents. ‘Document’ is defined in Part 1 of the Dictionary in the Act very broadly and includes electronic records.

Section 47(2) defines a copy of a document to include a document that is not an exact copy of the document but that is identical to the document in all relevant respects.

Section 48 enables a party to adduce evidence of the contents of a document by one of a number of means, including producing electronic copies of a document. Section 48 of the uniform Evidence Acts permits the tendering of a copy of a document produced ‘by a device that reproduces the contents of documents, enabling computer produced copies of documents to be admitted as evidence’ (s48(1)(d); Ogders 2004, para 1.2.4920). Section 48 permits the tendering of a document produced by a computer as evidence of the contents of the computer record (*R v Dudko* [2002] NSWCCA 336). In *R v Dudko* [2002] NSWCCA 336 printouts of detailed computer generated telephone audit trail records were admissible under s 48. Section 48 also permits a copy of a copy of a copy of an electronic record to be produced as evidence (*Lewis v Nortex Pty Ltd (In Liq); Lamru Pty Ltd v Kation Pty Ltd* [2002] NSWSC 337).

It should be noted that ss 48 and 51 do not affect the requirement to prove that a document that is tendered as evidence is the document that it purports to be (*NAB v Rusu* [1999] NSWSC 539; *Inspector Stephen Campbell v James Gordon Hitchcock* [2003] NSWIR Comm 148). It is still necessary when tendering a document to prove its authenticity.

The result of these provisions of the uniform Evidence Acts is that all documents are now admissible, however it is for the courts to determine the weight to be given to the documents (Davidson 1999, p29).

Admission of computer produced evidence

Sections 146 and 147 facilitate proof of ‘evidence produced by processes, machines and other devices’ and were intended to facilitate the admission of computer produced evidence (ALRC 2005, p143).

Section 146 provides that where a document or thing is produced wholly or partly by a device or process that ordinarily produces a particular outcome, it is presumed that the device produced that outcome on the occasion in question unless evidence to the contrary is raised. For example, it would not be necessary to call evidence to prove that a photocopier normally produced complete copies of documents and that it was working properly when it was used to photocopy the relevant document (ALRC 2005, p143).

Section 147 provides a similar rebuttable presumption in relation to documents produced by processes, machines and other devices in the course of a business, however under s 147 it is not necessary to show that it is reasonably open to find that the device ordinarily produces the particular outcome. Additionally s 147 does not apply if the contents of the document were produced for the purpose of conducting, or in contemplation of, or in connection with legal proceedings, or in connection with investigations relating to or leading to criminal proceedings.

Sections 146 and 147 relate to the requirement to provide evidence of the accurate working of the computer that generated the electronic record. This will be presumed if the requirements of the sections are met. It will still be necessary for the electronic record to be admissible either as real evidence, or under one of the other statutory exceptions to the hearsay rule.

In *Inspector Stephen Campbell v James Gordon Hitchcock* [2003] NSWIR Comm 148, the New South Wales Industrial Commission found that the Safe-T-Cam system of tracking heavy vehicle movements in New South Wales did not satisfy the requirements of s146 because the evidence suggested that the system was not 'foolproof' but required manual checking. On the facts of the case s 147 was also not available because the database was prepared in connection with criminal proceedings i.e. the alleged breaches of road laws.

These provisions of the uniform Evidence Acts facilitating the production of computer produced evidence do not include a rigorous process for ensuring the reliability and accuracy of the evidence (ALRC 2005, p144), but rather presume the accuracy of computer output.

It is still necessary for the content of documents tendered as evidence to be authenticated, for example in the case of computer records, it is necessary to give evidence that the computer output is what it purports to be (National Archives of Australia 2004).

Where authentication of a document is in issue, a court may make an order that (National Archives of Australia 2004):

- The original document be produced;
- A party be permitted to examine, test or copy a document;
- A person concerned in a record keeping system be called to give evidence; or
- In the case of a computer or similar document, that a party be permitted to examine and test the way in which the document was produced or has been kept.

5.2.6 Conclusion

Where a party seeks to have electronic records in relation to a construction project admitted as evidence in court proceedings, the key issues will be:

- Where the document contains a statement made by a human, for example an email or a project record, the hearsay rule may prevent the document being admitted as evidence unless one of the exceptions to the hearsay rule applies.
- The hearsay rule will not prevent an electronic contract from being admissible as evidence. However, it will be necessary to establish that the electronic copy produced in court is an accurate copy.
- If the electronic record is a book of account or a business record the hearsay rule is excluded and the document may be admissible. Many emails and project records will be admissible on this basis.
- Alternatively, in Queensland, an electronic record may be admissible as a document produced by a computer. In that case evidence of the proper working of the computer system must be provided, however, this can be done by a certificate.
- If the original record is a paper record and an electronic copy is produced as evidence, the electronic record may not be the best evidence available. However it is likely that the electronic record will be admissible under either ss 146 or 147 of the uniform Evidence Acts or under s 95 of the Queensland Act.
- Where an electronic record is a computer generated record (not containing a statement by a human), such as an audit log, it will be admissible as real evidence. In Queensland the four requirements of s 95 will still need to be satisfied for such evidence to be admissible.

Section 5.4 of this Report considers the application of these issues to particular documents that may be relevant to parties involved in construction litigation.

5.3 Weight

5.3.1 Introduction

While an electronic record may be admissible as evidence, it may be given less weight by the court than its non-electronic equivalent. The court may not necessarily believe or act on the evidence (National Archives of Australia 2004). The weight that will be given to electronic evidence will be dependant upon the security and management of the electronic storage system (DPWS 2000, p26). A review of the literature reveals that the following issues arise in connection to the weight to be given to electronic evidence:

- How can the integrity of electronic records be proven given the belief that they can be altered without trace or that data may have been corrupted due to a computer or software malfunction?

- How can the authenticity of the origin of electronic records be proved? In other words, how can it be shown that an electronic record has not emanated from a fraudulent source?

- How may the time of dispatch and receipt of an electronic communication be proved?

- How can the correct operation of hardware and software be proved?

- How can errors in electronic records be detected?

- If a printed version of an electronic record is admitted as evidence will it have less weight than the electronic record itself would have had?

- How may the chain of custody of evidentiary documents be proved?

5.3.2 Document integrity

Document integrity refers to whether or not a document produced in court as evidence is the same as the original document. Doubts arise because electronic records may be easily altered and such alterations may not be detectable. Laryea (1999, para 5) argues that the integrity and reliability of electronic evidence is viewed suspiciously by the legal community due to the notion that ‘electronic data is alterable without trace, easily corruptible, prone to hacking and can easily emanate from a fraudulent source (the sender pretending to be someone else).’ The reliability of electronic data may be impacted by viruses, data corruption, hackers and computer malfunctions (Laryea 1999, para 88). Thompson (2004, p133) argues that an email that is insecure in the sense that it is not authenticated and not encrypted, is likely to have little or no probative value as evidence.

Consideration should also be given as to whether the integrity of the meta-data associated with an electronic record is guaranteed. Meta-data may include information such as the origin and date of creation of the electronic record. The meta-data may reveal critical information without which the evidentiary value of the electronic record is reduced (Williams, 2005).

In Queensland there is no presumption as to the integrity of an electronic record. Where electronic records are admitted as evidence under s 95 of the *Evidence Act 1975* (Qld), a certificate may be given as to the correct operation of the computer. Under the uniform Evidence Acts, ss 146 and 147 provide presumptions as to the proper operation of the computer system. Neither the provision in the Queensland Act nor the provisions in the uniform Evidence Acts apply generally as to the integrity of an electronic record but are limited to the correct operation of the computer. Accordingly, it will be necessary both in

Queensland and under the uniform Evidence Acts for the party relying on an electronic record to prove the integrity of the document if it is called into question by the opposing party.

Despite doubts by Laryea (1999) about the weight which will be given to electronic records, the judicial cases to date do not indicate that the courts have had any difficulty accepting the integrity of electronic evidence. The cases suggest that unless objection is raised, the integrity of electronic evidence is accepted on its face (ALRC 2005, p150). Similarly, in the United States, courts are increasingly relying on the trustworthiness of electronic evidence and relying upon the opposing party to point out any flaws that may exist in the electronic evidence (Givens 2003/2004, p7).

There is a view that the integrity of electronic records should not be so readily accepted by the courts. The ALRC (2005, p150) suggests that 'the integrity of a document produced by a computer cannot be assumed and its probative value may have to be questioned.' Spenceley (2003) suggests that there is empirical evidence that presumptions of accuracy of computer produced material are often incorrect and that errors are not detected by physical inspection of the material. While issues connected to the integrity of electronic records have not generally been raised in litigation to date, it is possible that as lawyers become more familiar with the technical arguments that might arise, the integrity of electronic records will be challenged more frequently. In that case, the ability to show that an electronic information system is managed in accordance with recognised standards will be persuasive to the courts (Wilkinson 2005, p110). To ensure that electronic records are given the same evidentiary weight as other evidence, computer systems should be able to establish that electronic records have not been altered (DPWS 2000, p23).

Methods of establishing that an original record has not been altered include (Standards Australia 2003, pp 16-18):

- Retaining the original document in non-electronic form for comparison.
- Relying on computer operating systems and circumstantial evidence.
- Storing the original electronic record on write once read many (WORM) media.
- Cryptography (e.g. hash or MAC).
- Demonstrating that unauthorised persons or programs are prevented from altering the record and did not alter the record.

A further method of establishing that an electronic record has not been altered is where communications are monitored by a third party and the monitoring system records information about the message contents (Reed 2001, p92).

The technical means of ensuring the integrity of electronic records are considered in section 5.3.9 of this Report.

5.3.3 Authenticity of computer evidence

Authentication means identifying the author of an electronic record (data origin authentication) and may also include authenticating that the person is who they say they are (non-repudiation) (DPWS 2000, p11). Authentication is particularly an issue in relation to email where it is necessary to prove that the email was actually sent by the purported author. From an evidentiary point of view authentication is more than the recipient of the message merely being able to satisfy him or herself that the message originated from the sender; it also refers to the recipient being able to prove to a 'judge' that he or she did not forge the message (McCullagh, Caelli & Little 2001, p8).

Authentication is an issue in connection with emails because (Mallesons 2003):

- an email address may be obtained without proof of identity;

- emails may be sent from another person's computer without their permission;

- unencrypted email is relatively insecure, meaning that email recipients cannot be certain of the identity of the sender in the absence of a digital signature.

Section 15 of the ETA (Cth) and s 26 of the ETQA provide that unless otherwise agreed, a purported originator of a message will only be bound if the communication was sent with the authority of the purported originator. Accordingly, where either the ETA (Cth) or the ETQA apply, it is possible that the purported originator may deny authorship. Similarly at common law, a purported originator of a document can deny authorship (*Grayden* (1988) 36 A Crim R 163; *In re Piranha, Inc,* 297 B.R. 78 aff'd, 33 Fed. Appx. 19, 2003 U.S App. Lexis 24745).

Electronic records may be authenticated by either technical or non-technical means. Non-technical means involve proving by either direct or circumstantial evidence that the purported author of the message was in fact the author. Email may be authenticated by:

- The testimony of the author of the email or some other person who saw the email composed and transmitted (Robins 2003, p226).

- The email's contents and markers (Casamassima & Caplicki 2003). For example an email may contain facts known only to a particular person or the language patterns used may be peculiar to that individual (Robins 2003, pp227-8).

- Production of the email in response to a discovery request (Casamassima & Caplicki 2003).

- Other indicia of authenticity such as employee's notes, letterhead and the subject matter of the email (Casamassima & Caplicki 2003).

- Circumstantial evidence regarding access to the computer system at the relevant time may also assist in authentication. Such circumstantial evidence may be compiled from witnesses, video, building access systems, telephone records or latent forensic evidence (Standards Australia 2003, p15).

Potential technical means of addressing authentication concerns include (Standards Australia 2003, p15):

- userid and password;

- digital signatures;

- security tokens;

- smart cards, and

- biometrics.

Where a third party monitoring system records information about the identity of the sender and recipient of the message, that system provides strong evidence of the integrity and authenticity of electronic records (Reed 2001, p92).

The technical means of ensuring the integrity of electronic records are considered in section 5.3.9 of this Report.

5.3.4 Proof of time of dispatch and receipt

While the time and date an electronic record is created may be automatically recorded by the computer software applications in use, these records can be altered or manipulated by changing the relevant computer clock (DPWS 2000, p44). Computer clocks may also be inaccurate and there is no guarantee that different clocks will be synchronised. Potential means of proving the time of dispatch and receipt of a document are (Standards Australia 2003, p18):

- Time and date stamping by trusted third parties or internal time and date stamping; and

- Synchronisation of computer system clocks to a central reference.

At common law there appears to be a presumption of accuracy of clocks (*Gorham v Brice* 18 TLR 424; *Nicholas v Penny* [1950] 2 KB 466). The presumption was applied in relation to the use of clocks to record speeds of automobiles. However, in *R v Magoulias* [2003] NSWCCA 143, the New South Wales Court of Criminal Appeal said:

> It is a notorious matter of fact that reliable clocks or timing devices may show slightly different times. A clock may gain or lose ever so slightly and it may be some days before the difference becomes noticeable. When setting a clock or timing device there might be a very small error. Perhaps the clock from which the timing device is set is slightly astray. It is exceedingly well known that the timing of differing clocks needs to be synchronised if pinpoint accuracy is required.

It was argued in *R v Magoulias* that s 146 of the uniform Evidence Acts provides a presumption in favour of the accurate working of timing devices. The argument was not rejected by the Court, but on the facts of the case any such presumption was rebutted. Accordingly it will be open to argue that the correct operation of a computer clock can be presumed under the uniform Evidence Acts. In Queensland the common law position would apply so that it may be argued that there is a presumption as to the accurate working of computer clocks. However given the notorious inaccuracy of computer clocks it may be argued that either the presumption should not apply or it should be able to be easily rebutted in any given case where the accuracy of the computer clock is disputed. Accordingly, it may be necessary to use technological means to establish the date and time of creation or communication of an electronic record.

5.3.4.1 Digital time stamps

Digital time stamps are one means of establishing the time at which an electronic record is created or communicated. The issues that arise in relation to the use of time stamps include (BIICL 2006):

- What type of time stamp should be used?

- How accurate are time stamps?

- Should third party vendors be used?

- What standards should be observed?

What type of time stamp should be used?

A digital time stamp establishes the existence of an electronic record at a particular point of time. Time stamps are digital signatures created by a time stamping authority attaching the current time, date and identification of the owner to the hash value of the electronic record. The two properties that define the type of time stamp that can be used are the type of cryptographic algorithms and the format of the electronic data in which the time is recorded.

Cryptographic algorithms

The Australian Government Information Technology Security Manual (ACSI 33) (DSD 2006) specifies a set of cryptographic algorithms that must be used for the protection of communications with Australian Government departments and agencies.

The public key algorithms identified in the Manual are:

- Diffie-Hellman key agreement protocol (Diffie & Hellman 1976);
- Digital Signature Algorithm (DSA) (NIST 2000); and
- Rivest-Shamir-Adleman (RSA) encryption (RSA Laboratories, 2002).

The symmetric encryption algorithms identified in the Manual are:

- Advanced Encryption Standard (Daemen & Rijmen 2001); and
- Triple DES (NIST,1999).

The cryptographic hash functions SHA-1, SHA-224, SHA-256, SHA-384 and SHA-512 from the secure hash algorithm (SHA) family are recommended for hashing purposes (FIPS 2002).

It is also necessary to have cryptographic protocols that specify how the algorithms are to be applied to communications data and how cryptographic keys are derived. An example of a cryptographic protocol that specifies key establishment techniques based on symmetric keys and asymmetric keys is ISO/IEC 11770.1-3 (117700.1-3, 2004). A new standard ISO/IEC 11770-4 (ISO/IEC 2006) defines key establishment mechanisms based on weak passwords.

Secure Sockets Layer (SSL) may be used in order to ensure the confidentiality of an electronic record during transit to and from the time stamping authority. SSL is the most common standard for secure Internet communications (Freier et al.1996). The SSL protocol has two main stages. In the first stage, SSL uses public key cryptography and digital signatures to validate the server and ensure that the server is who it claims to be. Because there is no recognised public key infrastructure in place, the web browser will often require the user to verify the digital certificate manually. SSL does not authenticate the user. After the server has been authenticated, a symmetric key is selected for the session and symmetric key encryption is used to exchange information. For each transaction, a different encryption key is used. It is recommended that SSL be used for all secure communications required in the e-contracting process. However, it should be noted that SSL provides confidentiality and integrity on the communication network only. When the host machine receives the message or the file is uploaded, it is automatically decrypted. The information will not remain confidential once it is received unless the sender has encrypted the message by additional means.

Format of electronic data

Various standard formats can be used for the electronic data by which the time is recorded including:

- **ISO 8601** -an international standard for date and time representations which can be used to for time stamping purposes.
- **XML schema definition** (XSD) - used to describe and validate date and time in an XML environment. XSD defines a type of XML document in terms of constraints upon

what elements and attributes may appear, their relationship to each other and what types of data may be in them.

How accurate are time stamps?

The accuracy expected from a time stamp will depend on the purpose for which it is to be applied. For example, when using a time stamp to measure Web server response time, where sub second service time is expected, a high degree of accuracy is required. When a time stamp is used for electronic contracting or record keeping purposes, such a high degree of accuracy is not required.

The accuracy of a time stamp depends on the accuracy of the timeserver that allows the time stamping authority to synchronise its system clock over the Internet. The time information provided by the timeserver to a time stamping authority is directly traceable to the Universal Time Code. Accuracies of 1-50 milliseconds can be achieved using Network Time Protocol (NTPv3) depending on the characteristics of the synchronisation source (Mills 1992).

The methods by which time can be established accurately are discussed in section 5.3.4.2 of this Report.

Should third party vendors be used?

A time stamping authority issues time stamps that can prove the existence, integrity and authenticity of electronic data at a particular point of time. A time stamping authority can either be a part of the business organisation using the time stamp or a separate trusted third party whose only role is to issue time stamps.

A trusted time stamping authority should be used to issue and verify a time stamp if the time stamp may be of high evidential importance in the event of a subsequent dispute. In that case the trusted time stamping authority will enable fraud to be detected and proved to the court (Buldas et al. 2000). The trusted time stamping authority can either use its own product or third party products to generate time stamps. For example, Cryptomathic Time Stamping Authority (CTSA) (CTSA 2003) generates a unique and unforgeable time stamp that can be assigned to any piece of digital data using products from its specification and also supports third party vendor products.

What standards should be observed?

A relevant standard for the implementation of digital time stamps is Internet X.509 Public Key Infrastructure Time Stamp Protocol (Adams et al. 2001). This standard describes a time stamping authority as a trusted third party, which creates time stamps establishing the existence of data at a particular point in time. The standard anticipates that a time stamping authority will make known to prospective clients the policies it implements to ensure accurate time stamp generation, and clients will make use of the services of a time stamping authority only if they are satisfied that these policies meet their needs.

The security of the time stamp issued by a time stamping authority depends on the following general security properties:

- It must be infeasible for a time stamping authority to time stamp a document with a date and time that is different from the correct one.

- It must be infeasible to change even a single bit of a time stamped document without the change being apparent.

- Relative temporal authentication (Buldas et al. 2000) or temporal authentication (Just 1998a, Just 1998b), intuitively combines message authentication with the notion of timeliness of messages. A time stamping authority is said to provide relative temporal authentication if one is able to decide which stamp has been issued first for each pair of time stamp. This is achieved by applying a collision resistant hash function to the earlier stamps which is then incorporated in the later time stamp.

- The time stamping authority must be reliable and available when needed (Ansper et al. 2001). A time stamping authority may become unavailable for various reasons including a denial of service attack on its server due to the poor design of protocols. During any period of unavailability, the parties relying on the time stamping authority would not be able to obtain a time stamp for any electronic record which was required to be preserved. An obvious method of protecting against service interruption is the use of multiple servers (Ansper et al. 2001). This approach helps to keep time stamping services available and to restore the evidentiary value of time stamps if the keys are compromised or if the time stamping authority's database is lost.

5.3.4.2 Synchronisation of computer system clocks

Time can be established accurately by atomic clocks and may be distributed by systems such as Network Time Protocol (Mills 1992) and Simple Network Time Protocol (Mills 1996, 2006). Network Time Protocol provides a mechanism to synchronise time on computers connected over the internet. Network Time Protocol is highly accurate even where factors such as unreliable internet connections are involved. Simple Network Time Protocol is a reduced accuracy version of Network time Protocol which can be used when the ultimate performance of the full Network Time Protocol is not necessary or justified (Mills 2006).

5.3.5 Verification of correct operations

Under the Queensland Act, one of the requirements for computer produced evidence to be admissible is that there has been an absence of computer malfunction (s 95). Under s 95(4), evidence of an absence of computer malfunction can be given by a certificate signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities. Therefore prima facie if such a certificate is given the correct operation of the computer can be accepted. If evidence is given to the contrary it would be a matter for the party seeking to rely on the evidence to prove that there was an absence of computer malfunction. The certificate is merely evidence of the absence of computer malfunction and does not create any presumption in favour of the party seeking to rely on the evidence.

Under the uniform Evidence Acts, the correct operation of a computer system can be presumed under ss 146 or 147. It would therefore be for the party challenging the evidence to prove that the computer system was not working accurately.

If there is some evidence that the computer system is not working accurately, it may be difficult for the party seeking to have the electronic evidence admitted to overcome such evidence and prove the computer system was working accurately. Assuring high levels of reliability of complex information systems is a difficult and expensive engineering task. It requires methodological design and deployment, as well as detailed evaluation. A number of strategies can be taken to enhance the demonstrable reliability of the software and hardware to verify the correct operation of the system:

- Identify the particular components of the computer system which may impact on the evidential value of the record and limit the verification process to these components. This reduces the complexity of the verification procedure.

- Use certified products. There exist several security evaluation standards that are used by independent entities to assess the conformance of products to a set of standard security requirements. The two more common evaluation standards are the Information Technology Security Evaluation Criteria (ITSEC) (CEC 1991) and the Common Criteria (CC) (ISO 1999). Both standards define different levels of security testing, resulting in the levels of assurance. In Australia, the Defence Signals Directorate is the only accredited body for issuing certification according to the ITSEC and CC standards.

- Use trusted operating systems. Trusted operating systems, such as Sun Trusted Solaris of Sun Microsystems Inc., are certified according to ITSEC and CC standards, and provide strong assurance on the operating system access control mechanisms. This allows the protection of programs and data against unauthorised modification. Trusted operating systems can enforce strict security policies that restrict the capabilities of even system administrators. The use of these systems provide a level of trust that the system is functioning correctly.

As a result it is suggested that certified products or trusted operating systems should be used in the production and storage of any electronic records that may have evidentiary value.

5.3.6 Error detection

Spenceley (2003) suggests that there is empirical evidence that presumptions of accuracy of computer produced material are often incorrect and that errors are not detected by physical inspection of the material. Mechanisms of providing some verification that a computer failure has not occurred can involve software, hardware, human solutions or a combination of all three. An example would be manual checking of the output or comparison of the output produced by a parallel computer (ALRC 2005 p147, citing Spenceley 2003, p255).

5.3.7 Weight given to print outs

Section 146(2) of the uniform Evidence Acts provides that where a device or process ordinarily produces an outcome if properly used, it is presumed, unless evidence to the contrary is raised, that in producing the document or thing on the occasion in question the device or process produced the outcome. The Electronic Commerce Expert Group (1998, para 2.9.20) argues that this presumption addresses the weight to be given to the production of a hard copy of an electronic record.

The meta-data that is associated with an electronic record is likely to be considered part of the document and therefore should be produced as part of the documentary evidence. If the print out of the electronic record does not include the meta-data it may be of less evidentiary value. In the United States, in *Armstrong v Executive Office of the President* 810 F. Supp 335, it was held that where the court had ordered the preservation of email communications, the order was not complied with by the preservation of print outs of the emails alone. The electronic versions of the emails contained much information that would not show up on the printed form, including the date of transmission, the date of receipt, detailed list of recipients and linkages between messages sent and replies received.

Davidson (1999) argues that as a result of such differences between the electronic records and the print out, greater weight should be given to the electronic records. It is therefore essential that electronic copies of documents be kept rather than parties merely relying on print outs of documents as records.

5.3.8 Chain of custody

It will be necessary to demonstrate an audit trail connecting the copy of an electronic record produced as evidence to the original record (Reed 2001, p90). Standards Australia (2003, p22) argue that the evidentiary weight of electronic records will be substantially reduced if the chain of custody cannot be established. In order to establish a chain of custody organisations should:

- Create an evidence copy; and

- Maintain a custody log of the evidence copy.

In *Lewis v Nortex Pty Ltd (In Liq); Lamru Pty Ltd v Kation Pty Ltd* [2002] NSWSC 337 the electronic evidence in question were files stored on a floppy disk drive and the hard drive of a party's personal computer. The floppy disk had been stored in a drawer with other floppy disks and the personal computer had been lent to a business partner to use for children's games. The court criticised the custodian of the documents, however, the electronic records in question were ultimately accepted as being unaltered copies of the relevant documents.

5.3.9 Technical solutions

The technical issues that are of concern in relation to the admissibility and weight that is to be attached to electronic evidence are:

- Integrity: Can it be proven that the electronic record produced in court is the same as the original and has not been altered?
- Data Origin Authenticity: How can it be established that the electronic record has originated from the source from which it is purported to originate?
- How can the time of creation and communication of an electronic record be established? (Discussed in section 5.3.4.)
- How can the correct operation of the computer system be proven? (Discussed in section 5.3.5.)
- How will the parties or the court be alerted to the existence of errors in electronic records that would suggest the integrity or authenticity of the record should be examined? (Discussed in section 5.3.9.3.)

The literature reveals that the method most likely to be acceptable in ensuring both the integrity and data origin authenticity of an electronic record is a digital signature. The use of digital signatures to satisfy these requirements is discussed in section 5.3.9.1 of this Report. Other technological methods of ensuring integrity and data origin authenticity are discussed in section 5.3.9.2.

5.3.9.1 Digital signatures

The operation of digital signatures has previously been discussed in section 3.12.2 of this Report. In summary, the integrity of a document is assured by the use of the encrypted hash and the origin of the document is assured by the use of the private key. Where a digital certificate is used the identity of the originator of the document may be established by the certification authority.

There has been no judicial consideration as to whether a digital signature is admissible to prove the integrity or authenticity of an electronic record. Several evidentiary issues may arise in relation to a digital certificate:

- The certificate may be hearsay evidence as to the identity of the holder of the public key.
- The digital signature may have been compromised.
- The use of a digital signature does not prove who actually affixed it.
- A digital signature may have been stripped from the document and replaced with another digital signature.

Hearsay evidence

A certifying certificate may be hearsay evidence as to the identity of the holder of the public key (Mason 2002, p177). Digital signatures may be admissible under one of the statutory exceptions to the hearsay rule, however, there has not been any judicial determination of such admissibility (NOIE 2002, p59). The National Office of the Information Economy (2002, p55) identifies several factors that may impact on how much weight is given to a certificate as evidence of the identity of the holder of the public key. Doubts may be raised as to the accuracy of materials relied upon by the certification authority to establish the identity of the holder of the public key, and also as to the accuracy of the process by which the applicant for a public key is associated with the key.

Compromise of digital signature

A second means of attacking a digital signature may be that the certificate has been compromised (NOIE 2002, p56). One of the challenges of using digital signatures is to prove the validity of signatures well into the future when the signers or related CA's credentials are no longer valid or available (Chokhani & Wallace 2004). A party challenging the admissibility of the electronic signature may claim:

- The security used by the sender was not sufficient to prevent a third party from gaining access to the computer or system and making improper use of their key number (Mason 2002a. p178);

- The procedures and technical abilities of the trusted third party were at fault (Mason 2002a. p178);

- Another organisation in the chain that links the sending of the electronic key and its receipt by the relying party, other than the trusted third party was at fault (Mason 2002a. p178).

- A digital signature does not carry trustworthy information about the time when it was created. If the digital signature was created when the signer's certificate is no longer valid it will not verify the authenticity or integrity of the electronic record (SETCCE 2005).

- The cryptography upon which the digital signature is based may have become unreliable. Cryptographic algorithms that are used to provide security for electronic documents are inevitably exposed to various outside factors, thus becoming more and more vulnerable. For example, digital signatures and encrypted data that were produced using cryptographic keys of limited length are eventually becoming easier to break and cannot provide adequate long-term security (SETCCE 2005, Maniatis et al. 2001). The processing power of modern computers is rapidly increasing, making the cryptographic algorithms and encrypted data easier to break. For example, see the recent collision attacks on popular standard cryptographic hash functions such as MD4, MD5, SHA-0 and SHA-1 (Wang et al. 2004, 2005a, Wang & Yu 2005, Wang et al. 2005b,c, Xiaoyun Wang & Yao 2005).

- The private key of the signatory may have expired (Verisign 1998).

The probability of a private key being lost or compromised increases as time passes. To maintain the level of security at a sufficient level, cryptographic algorithms, and encrypting and signing keys are being replaced with stronger ones every few years. The NIST recommends phasing out the SHA-1 hash function (NIST 2005) which is used by many CA's in their digital certificates (Gauravaram et al. 2006), in favour of larger and stronger hash functions by 2010. According to the Public Key Infrastructure (PKI) policy, as stronger keys for encryption algorithms are generated and stronger cryptographic hash functions are used, new digital certificates have to be issued. In general, the maximum lifetime of an issued digital certificate is five years. As a consequence, all digital signatures that were applied to electronic contracts become null and void when the corresponding digital certificates expire. This holds true unless the respective electronic contracts had previously been processed in a way that the lifetime of their applied digital signatures has been prolonged. The validity of digitally signed electronic contracts can be extended over time using digital time-stamping. The use of digital time stamping is discussed in section 5.3.4 of this Report.

Proof of use of digital signature

According to Sneddon (2000, para 3.2(b)(i)), digital signatures can prove that an electronic signature was affixed to a communication, but they cannot prove who affixed the signature. The inference that the holder of the certificate affixed the electronic signature to the communication is weaker where there is inadequate security on the computer system on which the certificate sits. The party seeking to rely on the signature may need to produce extrinsic evidence that the signature was applied with the authority of the purported sender (Reed 2001, p96).

Digital signature stripping

A digital signature relying on use of a one-way hash and public-private key cryptography can be stripped from the document and replaced by an alternative digital signature. Such stripping would make it appear that the document has been sent by a person other than the actual originator (McCullagh, Caelli & Little 2001, p12). Therefore it is necessary that the recipient of a document can determine if a substitution of digital signatures has occurred. One method of preventing signature stripping would be to either encrypt the digitally signed document (so that the digital signature and the document are indivisible) or to use a trusted third party, most likely a certification authority, to verify the sender of the message (McCullagh, Caelli & Little 2001, pp14-15). Where a certification authority is used the identity of the sender is verified because the certification authority takes traditional evidence of the identity of the person to whom a certificate is issued (Reed 2001, p95). In that case, unless there is evidence to the contrary, a court should be satisfied that the purported signatory was the originator of the electronically signed document.

Mason (2002b, p244) argues that trusted third parties will need to guarantee that they can audit the evidential trail in relation to the use and control of the certifying certificates and key numbers they issue. The weight that will be given to the evidence relating to a digital signature will depend on the degree of control exercised over the controlled and secure environment of all the parties in the chain.

While the issues discussed above may place doubt on the validity of digital signatures, it is arguable that digital signatures are in fact more difficult to forge than manuscript signatures (Reed 2001, p96).

5.3.9.2 Other methods of ensuring integrity and authentication of origin

As discussed in section 4.5.9 of this Report, authentication may be achieved by relying on one or more of the following methods (NOIE 2002):

- Something the user knows, such as a password or a personal identification number (PIN). This assumes that only the owner of the account knows the password or PIN needed to access the account.

- Something the user has, such as a smart card or token. This assumes that only the owner of the account has the necessary smart card or token needed to unlock the account.

- Something the user is (biometrics), such as fingerprint, voice, retina, or iris characteristics of the user.

The authentication method used will depend on the degree of assurance required in relation to the transaction. While using a combination of these methods (such as a security token combined with a one off password) may achieve a high level of assurance of authentication of the origin of the electronic document, none of these methods will establish the integrity of an electronic document except in so far as they can establish that no person had access to the record in order to alter it.

5.3.9.3 Error detection

Any compromise of integrity of electronic records can be due to two factors:

- Alteration of records due to errors introduced by the communication channel during the transmission of electronic records;

- Alteration of records by a malicious attacker in the communication channel aiming for some malicious means, such as forging records or masquerading the sender or receiver in the transmission.

Error detection is a set of techniques that can be used to detect the errors in message transmission. It is the ability to detect errors that are made due to noise or other impairments in the course of the transmission from the transmitter to the receiver to maintain integrity of the data transmitted. For example, contracts that are in transit during the contract negotiation phase may be corrupted due to impairments in the communication channel.

Checksum and cyclic redundancy check (CRC) are the two most common error detection techniques used to detect the errors in messages. In the checksum method of error detection, each transmitted message is accompanied by a numerical value based on the number of set bits in the message. The receiving station then applies the same formula to the message and checks to make sure the accompanying numerical value is the same. If not, the receiver can assume that the message has been garbled (Webopedia 2006).

In the CRC method of detecting errors, transmitted messages are divided into predetermined lengths that are divided by a fixed divisor. According to the calculation, the remainder number is appended onto and sent with the message. When the message is received, the computer recalculates the remainder and compares it to the transmitted remainder. If the numbers do not match, an error is detected (Webopedia 2006). Neither CRC nor checksum mechanisms provide strong integrity services for messages communicated over an insecure medium.

Message authentication codes (MACs) relying on symmetric key cryptography are mechanisms used to provide strong integrity for messages communicated over an insecure medium against malicious adversaries. Their purpose is to verify the integrity and authenticity of the message communicated over an insecure medium. A MAC function accepts an arbitrary length message to be authenticated as input along with a secret key shared among the users and outputs a unique MAC value also called an authentication tag. The MAC value protects both the integrity and authenticity of a message by allowing the receivers of the message to detect any changes to the content of the message. For a presented electronic record, a MAC function can be used to detect any changes to the record both by the creator and verifier of the record with their shared symmetric key used in computing the MAC value.

The security goal of a MAC function is to prevent forgery. That is, it must be difficult for anyone to compute the MAC value for a message without knowing the secret key. They differ from digital signatures, as MAC values are both generated and verified using the same shared secret key. That is, the sender and receiver of information must agree on the secret keys before initiating communications. That is why MAC functions do not provide the cryptographic non-repudiation security property offered by digital signatures. Any user who can verify a MAC is also capable of generating MACs for other messages. In general, MAC functions are designed from cryptographic primitives such as hash functions as in the case of HMAC (Bellare1996) or from block cipher algorithms as in the case of OMAC (Iwata 2003), CBC-MAC (Bellare 2000) and PMAC (Black 2002).

Digital signatures are recommended over MAC functions for electronic contracts as digital signatures achieve the cryptographic non-repudiation security property, which is not provided by MAC functions. In the context of electronic contracting, the cryptographic non-repudiation security property is quite important as the parties involved at any stage of the electronic contract life cycle cannot later deny or repudiate their actions in relation to the contract at any stage of the electronic contract life cycle.

5.4 Documents commonly used in the construction industry

As can be seen from the previous discussions, the rules as to the admissibility of electronic records as evidence are complicated. The primary objection that may be raised to the admission of electronic records is the hearsay rule, which applies when the records contain statements made by humans and the record is sought to be admitted as proof of the truth of the statements. Where a print out of a document is produced it might also be argued that the print out is not the best evidence available and that the electronic version of the document should be produced.

Whether or not a particular electronic record is admissible will depend upon what type of document is involved. This section considers some examples of the various types of documents that are commonly used in the construction industry and whether they may be admissible as evidence if they are created or stored electronically.

5.4.1 Emails

Email is used extensively in the construction industry and can provide a wealth of information for use during construction litigation. As noted by Casamassima and Caplicki (2003, p16):

> E-mail can be used by project managers reporting back to the home office, superintendents distributing meeting minutes, contractors requesting information from designers, architects and engineers exchanging ideas about overcoming obstacles, owners discussing matters with contractors, contractors discussing matters with subcontractors, or subcontractors contacting their suppliers about shipment dates.

An email will not be admissible as evidence of the truth of any statements made by the author of the email, unless one of the exceptions to the hearsay rule applies. One relevant exception to the hearsay rule is the business records exemption. An email may be admissible as a business record if it is part of the ordinary undertaking of the organisation. An email was admitted under the business records exception under the uniform Evidence Acts in *Rickard Constructions Pty Ltd v Rickard Hails Moretti Pty Ltd* [2004] NSWSC 984. An email will not be admissible under the Queensland Act if the maker of statement contained in the email does not give evidence, unless that person is unavailable to give evidence (because for example, they are no longer alive or they are interstate).

It is not clear whether an email will be admissible under s 95 of the Queensland Act as a document produced by a computer. It may be argued that s 95 only applies to documents that are generated by computers rather than documents that are stored by computers (Reynolds 1994). The only judicial consideration of this issue to date in *Mehesz v Reman* (1980) 26 SASR 245 suggests that the section would apply to computer stored as well as computer generated records. While the situation is unclear, it is arguable that emails are admissible in Queensland under s 95. There is no equivalent to s 95 under the uniform Evidence Acts.

Where a print out of an email is sought to be introduced as evidence then the best evidence rule may well apply. If the print out does not include all relevant information such as the meta-data associated with the email it may not be admissible as evidence in Queensland. A print out will be admissible under s 147 of the uniform Evidence Acts, however the weight to be attached to the email as evidence may be reduced if the original electronic record is not produced (Davidson 1998, p29).

It will still be necessary to authenticate that the email has been sent by the person who is the purported author. Authentication may be of particular concern for emails as it is possible for an email address to be obtained without proof of identity and emails may be sent from a person's computer without their permission (Mallesons 2003). Under the uniform Evidence Acts, s 71 will enable the information contained in the email identifying the sender to be used as evidence of the identity of the sender. There is no equivalent provision in the Queensland Act and accordingly, the hearsay rule may prevent the use of the email itself to identify the sender.

An email can be authenticated by the various technical and non-technical means discussed in section 5.3.3 of this Report.

The integrity of an email may also be questioned. Integrity of electronic records generally is discussed in section 5.3.2 of this Report. Particular issues in relation to the integrity of emails are that changes may be made to the email prior to or after receipt without detection, access may be gained to the email or to the server by an unintended party, and unencrypted email is relatively insecure (Mallesons, 2003). As discussed in section 5.3.2 of this Report, courts have generally accepted emails as evidence without questioning their integrity. However it is possible that in the future lawyers will take issue with the integrity of emails and it may be necessary to bring evidence to establish that the copy of an email produced in court is in fact an accurate copy of what was actually sent. The methods of establishing the integrity of electronic records are discussed in section 5.3.9 of this Report.

The other issues regarding the weight to be attached to an electronic record as evidence of a contractual variation or notice (as discussed in section 5.3 of this Report) and the method of storing electronic records (as discussed in section 5.6 of this Report) will also be relevant.

5.4.2 The terms of a construction contract, notices and contract variations

Where documents are used in evidence to prove the terms of a contract, or that a notice has been given under a contract, the hearsay rule does not apply. Accordingly, such documents will be admissible.

It will still be necessary in relation to notices and contract variations to prove that the copy of a document provided to the court is an accurate copy. If a notice has been given or a variation made electronically, there may be an issue where a printout is given as evidence rather than the original electronic version of the document. Under the uniform Evidence Acts the print out will be admissible under s 146. The position under the Queensland Act is unclear, however the print out may be admissible under s 97 (Davidson 1999, p29). In either case the weight to be attached to the print out may be reduced if the print out does not include all of the information that is accessible from the electronic record.

The other issues regarding the weight to be attached to an electronic record as evidence of a contractual variation or notice (as discussed in section 5.3 of this Report) and the method of storing electronic records (as discussed in section 5.6 of this Report) will also be relevant.

5.4.3 Project records

The project records used in a construction project will be extensive and will form the basis of the evidence to be relied upon in most construction litigation. The project records include minutes of meetings, requests for information and reports of supervisors. Regardless of whether these records are kept electronically or in paper format, they will not be admissible unless they fall within one of the exceptions to the hearsay rule. Where these records are kept electronically additional issues may arise with respect to the weight to be attached to the records as evidence.

The types of records that have been admitted as business records are broad and the weight of authority would suggest that project records are likely to be admissible under the business records exemption as they will be part of the record of the undertaking.

Where the original project record is in paper format and a copy of the record has been made electronically there will be an issue as to whether the electronic record is the best evidence available. Under the uniform Evidence Acts it may be argued that where a scanned copy of a paper document has been stored electronically, then the electronic version or a later produced print out will be admissible under ss 146 and 147. There is no equivalent provision under the Queensland Act, however s95 may be able to be relied upon. There has been no judicial determination of this issue to date and it would be prudent where the original record is in paper format for the original record to be kept for evidentiary purposes. In any event it will still be necessary to authenticate that the document produced in court is an accurate copy of the original document if its authenticity is disputed.

Where the original record has been created electronically then the electronic record will be the best evidence available. In that case there may be an issue with regard to the admissibility of a print out of the record. The issues in relation to the evidentiary value of a printout of a project record will be the same as those for a print out of an email as discussed in section 5.4.2 above.

The other issues regarding the weight to be attached to an electronic record as evidence of a contractual variation or notice (as discussed in section 5.3 of this Report) and the method of storing electronic records (as discussed in section 5.6 of this Report) will also be relevant.

5.4.4 Financial records

The financial records of a construction project will include ledgers, job costs, invoices and labour records. These records will be admissible as either business records or books of account. Generally, the same issues will apply to financial records as apply to project records.

In addition, where financial records are kept electronically then the documents may be admissible under s 95 of the Queensland Act as a document produced by a computer.

5.4.5 Audit trails

Where documents are stored and produced by computers the computer system may keep audit logs tracking the date and time of creation of the documents, the author of the documents, access to the documents and any alterations that have been made to the documents. It may be necessary to use an audit log as evidence to establish or dispute the integrity or authenticity of an electronic record.

An audit log is produced by computers without human intervention other than in the programming of the computer. Such a record will be admissible under the common law exception to the hearsay rule as a document produced by a scientific instrument (*Rook v Maynard* (1993) 2 Tas R 97). It will also be necessary to bring evidence of the accurate working of the audit log program. This evidence may be given by the computer programmer or by the operator of the program.

5.4.6 Conclusion

Parties who are proposing to undertake electronic administration of construction contracts should ensure that an electronic records management system is established that maximises the evidentiary weight of the electronic records (Standards Australia 2003, p13). The electronic records management system should include procedures or technological methods that will:

- Ensure that the integrity of documents, including meta-data, can be proven;
- Ensure that the authenticity of electronic records can be proven;
- Enable the time of dispatch and receipt of electronic communications to be proven;
- Ensure that the correct operation of the computer system can be proven;
- Ensure that any errors are detected;
- Ensure that electronic copies of records are maintained even if printouts of such records are kept; and
- Demonstrate an audit trail connecting the electronic record produced as evidence to the original record.

5.5 Discovery

5.5.1 Introduction

The aim of discovery is to provide parties to litigation with access, prior to trial, to all relevant documentary evidence in each other's possession (White 2001, p47). Each party produces a list of documents in its possession verified by affidavit and must produce the documents for the other party's inspection unless they can claim privilege (White 2001, p47). Construction projects generate large numbers of project records that are relevant to litigation and which must be produced for discovery.

5.5.2 Discovery issues

A review of the literature reveals that the following issues arise in connection with the discovery of electronic records:

- Whether the electronic record is a document that should be discovered;
- When electronic records may have become 'unavailable' for discovery;
- Whether a court will make an order for discovery of electronic records if to do so would place an undue burden on the discovering party;
- Whether parties have complied with their duty to preserve evidence;
- The ease with which electronic records can be identified and retrieved; and
- Whether electronic records that have been deleted can be recovered.

5.5.3 Definition of 'document'

Electronic records are documents for the purposes of both the *Evidence Act 1977* (Qld) and the uniform Evidence Acts. Document is defined in Schedule 3 of the *Evidence Act 1977* (Qld) to include any disc or other device in which data are embodied so as to be capable of being reproduced and any other record of information whatsoever. The Dictionary in the *Evidence Act 1995* (Cth) provides that 'document' means any record of information and includes anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them or anything from which sounds, images or writing can be reproduced with or without the aid of anything else.'

In *Sony Music Entertainment (Australia) Ltd v University of Tasmania* [2003] FCA 532, the Federal court found that the definition of document included CD ROMs, tapes and other electronic storage devices and that the court had authority to order discovery of the devices notwithstanding that they may contain documents not otherwise discoverable, in other words, the definition of document was the whole storage device not individual files.

In *Paxus Services Pty Limited v People Bank Pty Ltd* (1991) 20 IPR 79, document was defined to include any record of information and therefore electronic databases for the purposes of the Federal Court Rules. It is clear that electronic records are documents which the parties may be obliged to discover and that the vast majority of electronic records in the possession of a party to litigation will be discoverable documents provided they are relevant to the dispute (Naismith 2003, p185).

Examples of electronically stored information that have been the subject of notices of discovery include (Gorry 1997, p61):

- Email (*NT Power Generation Pty Ltd, v Power and Water Authority* [1999] FCA 1669);
- Internally circulated electronic public announcements;
- Laser printer copies from optical discs;
- Electronic interchange message logs;
- Computer backup files *BT (Australasia) Pty Ltd v State of New South Wales (No 9)* [1998] 363 FCA; *Sony Music Entertainment (Australia) Ltd v University of Tasmania* [2003] FCA 532*;*
- Word processing files (*Alliance and Leicester Building Society v Ghahremani* [1992] RVR 198);
- Financial reporting systems (*Church of Scientology Inc v TCN Chanel 9 Pty Ltd* (NSW), referred to in Gorry 1997, p61);
- Document management audit trails;
- Databases (*Paxus Services Pty Limited v People Bank Pty Limited* (1991) 20 IPR 79); and
- CD ROMs, tapes and other electronic storage devices (*Sony Music Entertainment (Australia) Ltd v University of Tasmania* [2003] FCA 532).

The management of construction projects involves a large number of communications and documents which will be relevant to any construction litigation. Given the broad range of electronic records and storage devices that have been held to be discoverable, where these communications in relation to a construction project occur electronically, the task of providing discovery of all relevant documents may be onerous.

5.5.4 ‘Unavailable’ documents

A document that is ‘unavailable’ need not be discovered in court proceedings. A document is unavailable if (amongst other things) (Gorry 1997, p61):

- It cannot be found after reasonable enquiry and search by the party;
- It was destroyed by the party or by a person on behalf of the party, otherwise than in bad faith, or was destroyed by another person; or

- It would be impractical to produce the document or thing during the course of the proceedings.

While paper records may be destroyed without trace and therefore be unavailable, it is difficult to destroy an electronic record without leaving some trace of its existence either in back up media, third party systems or retained records of deleted files found on hard drives (Givens 2003/2004, p2). It is less likely that an electronic record will fulfil the criteria of being unavailable given the possible methods of traceability and recovery. Therefore a party may be obliged to make discovery of deleted electronic records if they are able to be recovered. Such a requirement may significantly add to the cost of compliance with an order for discovery.

5.5.5 Burden of complying with an order for discovery

As a general principle, courts will avoid making a discovery order that places an oppressive burden on a party such that it must devote disproportionate resources to the search for relevant documents (Naismith 2003, p183). In *Harman v Secretary of State for the Home* Department [1983] 1 AC 280 at 380 the court said:

> … the processes should not be allowed to place upon the litigant any harsher or more oppressive burden than is strictly required for the purpose of securing that justice is done.

This principle was cited with approval in Australia by Spender J in *Mackay Sugar Co-Operative Association Ltd v CSR Sugar Ltd* (1996) 137 ALR 183 at 187.

White (2001, p47) argues that this rule will enable parties to request that, where there is a vast quantity of electronic records, the scope of inquiry in relation to electronic records be limited to avoid great expense of recovery of data where there is little chance of useful information being obtained.

However, Naismith (2003, p183) argues that the mere fact that there is a large number of electronic records will not be enough to limit discovery. In *Oberdan v Commonwealth Bank* (1995) 75 SASR 152, the court said that an order 'will not be oppressive merely because the party to make the discovery is a large corporation; the issues are complex and the relevant events occurred over a long period'. This principle would seem to be relevant to a discovery involving a large number of electronic records.

In *NT Power Generation Pty Ltd v Power & Water Authority* [1999] FCA 1669, it was held that the party was required to discover all email communications and not merely those which existed in hard copy. The fact that discovery of email communications retained only electronically would involve considerable time, expense and effort did not excuse the party from giving discovery of them. Parties may well be ordered to make discovery of electronic records even though to do so may be time consuming and costly. It is therefore incumbent upon parties to ensure that electronic records are managed in such a way as to minimise these costs.

5.5.6 Duty to preserve evidence

Parties have a duty to preserve information that they know is relevant to ongoing or potential litigation (Naismith 2003, p186). Electronic records can be inadvertently destroyed by normal practices such as routine maintenance. As soon as litigation has commenced parties have a duty not to destroy relevant evidence (White 2001, p48). The duty may also extend to preserving documents even though litigation has not yet commenced.

In *McCabe v British American Tobacco Australia Services Ltd* [2002] VSC 73 it was held by the Victorian Supreme Court that BAT had illegally destroyed documents even though litigation had not yet commenced. The court held that records should be kept even when litigation has not commenced, where it would be reasonable to assume that there may be litigation. The ad hoc destruction of records for the purpose of hampering a case was held to be a criminal action. As a result of the destruction of documents Eames J ordered that BAT's defence be struck out. The decision was overturned on appeal in *British American Tobacco Services Ltd v Cowell* (2002) 7 VR 524 on the basis that the destruction of records was for the purpose of using records storage space more economically rather than an attempt to pervert the course of justice. In *R v Ensbey; ex parte A-G (Qld)* [2005] 1 Qd R 159 it was held by the Queensland Court of Appeal that a party cannot destroy a record if it believes that the record may be needed as evidence in possible future litigation. As a result of these two decisions, it is apparent that the duty to preserve evidence can arise prior to litigation actually commencing.

In order to comply with the duty to preserve evidence, parties have a duty to preserve back up media, make mirror images of hard drives and implement other steps to ensure that discoverable and relevant documents are preserved (Walters & Wright 2005). In *BT (Australasia) Pty Ltd v State of New South Wales (No 9)* [1998] 363 FCA, Telstra had been ordered to provide discovery of several classes of documents including employee emails. Telstra's usual practice was to back up information from its servers onto magnetic tapes which were overwritten periodically until they were no longer useable and were destroyed. Telstra was in breach of its discovery obligations by not taking steps to prevent the overwriting of back-up tapes.

Failure to preserve information relevant to litigation may result in prejudicial orders against a party in relation to costs or factual matters, or in the party being guilty of the tort of spoliation of evidence. Spoliation is the destruction or significant alteration of evidence, or the failure to preserve property for another's use as evidence, in pending or future litigation (Ballon 1998, p9). In the United States decision of *Linnen v A H Robins Company Inc* No 97-2307 (Middlesex Super Ct, 15 June 1999) a defendant failed to produce email back up tapes that were in its possession in relation to other litigation and also failed to revoke its back up tape destruction policy for four months after litigation commenced resulting in emails being unavailable. The court made an order against the defendant in relation to the costs of electronic discovery and also ordered that 'a 'spoliation inference' instruction would be given to the jury, permitting it to infer that the party which had destroyed potentially relevant evidence did so because it was unfavourable.' (Geiger 1999, p81)

The sanctions for spoliation in the United States include entry of default judgment, an adverse inference (i.e. an inference that the destroyed evidence would have been adverse to the destroying party's interests) or a costs order (Ballon 1998, p8). It is also possible that the court may order that the destroyed records be reconstructed (Howie 2005, p4).

Naismith (2003, p186) argues that the tort of spoliation of evidence does not form part of Australian law. Even if there is not a separate tort of spoliation the failure to preserve evidence may result in an adverse costs order, an adverse inference order or in extreme cases that a party's defence be struck out.

The routine destruction of electronic records pursuant to a records management system would not ordinarily amount to spoliation (Ballon 1998, p9). Stanfield (2005, p12) suggests that "if documents have been destroyed, perhaps in accordance with a routine document destruction policy, then as long as a litigant can show what was destroyed and when, that will stand the litigant in good stead in the court's eyes." Naismith (2003, p187) argues that an electronic records management system must include procedures to be followed in the event that litigation is anticipated. Such procedures would include the suspension of disposal practices and may also include saving a back-up at the commencement of litigation.

5.5.7 Retrievability and identifiability

The discovery process in relation to electronic records may be complex and expensive in light of the quantity and variety of electronic records that may be discoverable (White 2001, p46). Therefore a good electronic records management system should be in place to minimise time and money spent in the discovery process. Electronic records may be stored on the author's computer hard drive, the file server and router and the recipient's hard drive as well as on any back up media even after deletion. Records may also be stored on the author's or recipient's lap top, home computer or personal digital assistant and on removable storage devices such as CD ROMs (Naismith 2003, p188). Some copies of electronic records may be created by computers without the knowledge of the operator and these documents may not be recoverable without significant technical expertise. There is an obligation to discover all copies of documents, therefore, all of these multiple versions of electronic records will be discoverable (White 2001, p46). As a result, compliance with electronic discovery obligations can be expensive and time consuming. It is therefore essential that a party's system for management of electronic records enables documents to be easily identified and retrieved. It is also advisable that where there is an electronic records management system in place employees should be trained to use that system rather than relying on alternatives such as personal email or file directories.

To assist with the identification of relevant electronic records, it is recommended that electronic contracting systems not allow users to delete electronic contracting documents. Instead, users should be given the option to archive documents. These archived documents may then be stored and backed up outside of the electronic contract system. Other procedures should be put in place to ensure that documents are recoverable in the case of malicious attack or hardware failure.

5.5.8 Recovery of deleted documents

If electronic records have been deleted in the usual course they may not be discoverable. However, where deleted documents are retrievable because the data itself has not yet been deleted from the computer or is still available on back up media, then those documents are discoverable (Naismith 2003, p188).

Deleted records may be obtainable from back up media. If this is the case the back up media must be discovered. If an electronic record is not obtainable from back up media then the existence of the electronic document should be noted in the list of documents as a record once but no longer in the company's possession (Gorry 1997, p62).

If a company routinely deletes its email back up media and the media is destroyed prior to the company becoming aware of potential litigation, then those documents will be unavailable (Gorry 1997, p62).

White (2001, p49) argues that organisations in litigation prone industries should have established procedures to delete electronically stored documents from back up media. The purpose of such a policy is to reduce the burden of discovery rather than to destroy possibly incriminating evidence. Organisations should beware of falling foul of their obligations to preserve evidence discussed in section 5.5.6 of this Report. However it is unlikely that records destroyed in accordance with a valid disposal authority would be considered to be destroyed with the intention of spoiling a litigant's case (National Archives of Australia 2004).

Even where electronic records have been destroyed in accordance with a valid destruction policy, they may still be discoverable if it is possible to recover the deleted documents. There are powerful software tools available for computers that can restore deleted files (for example, contract files), find hidden files, and interface directly with computer hardware, bypassing the operating system (NIST 1995). In addition, deleted electronic documents may be stored on backup media for several days, weeks or months after they are deleted. In this event the back up media will be discoverable and should not be destroyed if they are relevant to potential litigation.

5.5.9 Conclusion

Electronic records and storage devices such as CD ROMs and computer hard drives will be documents that must be discovered if they are relevant to a dispute. Accordingly, organisations should adopt appropriate electronic records management systems in order to ensure that:

- Compliance with an order for discovery is not too expensive and time consuming.

- Electronic records that have been lawfully deleted in accordance with the policy are permanently destroyed so that they cannot be recovered and will therefore be unavailable for discovery.

- They are not found to have destroyed evidence relevant to anticipated litigation.

5.6 Preservation of electronic records

5.6.1 Legal requirements to preserve records

Obligations to retain and archive electronic records are found in various Commonwealth and State Acts. In particular, as a result of the *Limitations of Actions Act 1974* (Qld), in most cases organisations should keep electronic records for at least 6 years to defend or bring proceedings in relation to breach of contract or possible tort claims.

There are various other Commonwealth and State Acts that require organisations to retain records including:

- The *Income Tax Assessment Act 1997* (Cth) requires records to be kept for 5 years and 'to be readily accessible and convertible into writing in the English language'. The Australian Taxation Office has stated that it requires electronic records to be kept 'in such a way that the integrity of the content at capture, storage and reproduction stages can be demonstrated.' (Argy 2006)

- The *Corporations Act 2001* (Cth) requires companies to keep written financial records for 7 years after completion of the transactions covered by the records (s 286). Section 288 of the Act provides that if records are 'kept in electronic form, they must be convertible into hard copy. Hard copy must be made available within a reasonable time.'

The ETA (Cth) and the ETQA provide that where documents or communications are required to be retained they can be retained electronically provided certain conditions are met (ETA (Cth), s 12; ETQA ss 20-21). The main criteria within both of these sections are:

- The information must remain accessible; and

- The method used for storing information must be reliable for maintaining the integrity of the document.

Additionally where a public authority is a party to the contract the *Public Records Act 2002* (Qld) will require the public authority to keep and maintain public records. Section 14 of the Act requires that where records are kept electronically, they must remain able to be produced.

The provisions of ETQA must be complied with by public authorities in meeting their obligations under the *Public Records Act 2002* (Qld). Public authorities must also comply with Information Standard 40 (IS40). The Queensland Government *Best Practice Guide to Recordkeeping* (2003) provides assistance to public authorities in determining what is sufficient to meet their obligations under the Act and how to implement the policies and principles of IS40.

5.6.2 Technological issues in relation to the preservation of electronic records

The literature reveals that the key technological issues regarding the retention of electronic records are:

- Durability of storage media; and
- Readability of records.

Generally, parties will not be found to have satisfied their obligation to preserve records if the mechanism on which it is stored has broken down or if the record is saved in a format that is no longer able to be read by contemporary computer systems.

5.6.2.1 Durability

A potential problem in storing records electronically is that the storage medium may break down over time. The most common medium for archiving electronic records is the CD_ROM format which is considered more resistant to degradation than magnetic tapes and disks (NOIE 2002, p52). Environmental factors such as light, humidity and magnetic fields may also affect the durability of the storage medium (NOIE 2002, p52).

5.6.2.2 Readability

As technology changes it may be impossible to access documents stored on an outdated storage device. For example, back up storage tapes previously used larger spooling devices and older tape backups are not readable without specialised equipment (White, 2001, p46). Accordingly, good maintenance procedures are required to ensure that both the hardware and software by which electronic records are stored do not become superseded.

The three key strategies for ensuring electronic records remain readable in the future are technology preservation, migration and emulation (Digital Preservation Coalition 2002). Technology preservation involves retaining the appropriate software and hardware to ensure future access to archived electronic records (NOIE 2002, p54; DPWS 2000, p23).

Migration is a process of converting a document from an old format to a new format as technology evolves (Lynch 2004, p612). The method used to migrate an electronic record to a new technological environment should take into account the following considerations:

- There should be minimal loss of functionality of the electronic record (NSW Department of Public Works and Services 2000, p23).
- The authenticity and integrity of the electronic record should continue to be guaranteed (NSW Department of Public Works and Services 2000, p23).
- Important information such as formatting, structural components and meta-data should be preserved in the migration process.
- If a digital signature is used, the digital signature may have become degraded or obsolete and there may be a need for the digital signature also to be migrated (BIICL 2006). Accordingly, as part of the migration process it will be necessary to ensure that digital signatures and time stamps are also renewed in order to prolong their validity (Aalberts & van der Hof 2000; Dumortier & van den Eynde 2002).

Emulation involves building software on modern computers to enable the computer to ‘emulate’ old computers and read obsolete electronic records (Lynch 2004, p613). Problems that can arise with emulators include difficulties in communicating with storage and display devices that are complex to emulate and difficulties in emulating in a network environment.

An issue with respect to all three strategies is to ensure intellectual property rights in both the software and the electronic record will not be infringed (Digital Preservation Coalition 2002).

5.6.3 Conclusion

An electronic records management system should satisfy certain key criteria in order to ensure that the electronic records are admissible as evidence and have the same weight as non-electronic records, that parties can efficiently comply with an order for discovery and that their legal obligations to retain records are satisfied. A review of the relevant law and literature reveals that the issues to be considered are:

- If it is necessary to establish the proper working of a computer system for evidentiary purposes, what steps can be undertaken to achieve this?

- For evidentiary purposes it is important to establish that an electronic version of a document that is produced in court is the same as the original document. How can the authenticity of an electronic record in this sense be established?

- How can the integrity of an electronic record be verified if it is challenged in court so that the weight to be attached to the evidence will not be affected.

- How can it be established that the apparent origin of an electronic document is accurate? For example, in the case of an email, that the purported sender of the email did in fact send the email.

- How can the time of creation of a record or the time at which it was communicated be established with reasonable accuracy? This may be of particular importance in order to establish the time at which a notice under a contract was given. It may also be of importance in examining the accuracy of computer audit logs.

- What electronic records management system can be used to ensure that electronic records are readily identifiable, retrievable and able to be read at a later date, so that obligations in relation to discovery and the retention of records can be met?

- A policy in relation to deletion of electronic records should be put in place to ensure that documents that are required to be preserved for discovery or other legal purposes are not deleted.

6. CONCLUSION

This Report has identified a range of legal and security issues that may arise in connection with the formation, administration and recording of construction contracts within an electronic environment. A high level summary of the issues that have been identified is set out in the table below.

Summary of issues identified in this Report.

Contract stage	Identified issues
Electronic contract formation	• How can the parties to a construction contract avoid the legal uncertainties that arise when determining the precise point in time that an electronic contract has been formed? • What provisions should be included in a construction contract to minimise the legal relevance of the place where the contract is formed? • If the parties to a construction contract wish to administer their contract in an electronic environment, what communication protocols should be established at the time of contract formation to minimise the occurrence of inadvertent mistakes in the administration process? • What steps may be taken to minimise the possibility that an electronic guarantee may be unenforceable if it is not in writing and signed?
Electronic contract administration and management	• How can contracting parties address the risk that an exchange of electronic communications may, depending on terms and conditions the contract, have the effect of varying the contract? • What provisions may be incorporated into a construction contract to deal with the validity of electronic notices under the contract? • In relation to online collaboration platforms: o how can practical concerns such as the availability of the platform and exclusive use of the platform for project communications and records be ensured? o what provisions should be incorporated into the contract between the service provider and the project participants? o what technical standards should be established to ensure security, confidentiality and access control?
Electronic records management	• If it is necessary to establish the proper working of a computer system for evidentiary purposes, what steps can be undertaken to achieve this? • For evidentiary purposes it is important to establish that an electronic version of a document that is produced in court, is the same as the original document. How can the authenticity of an electronic record in this sense be established? • How can the integrity of an electronic record be verified? • How can it be established that the apparent origin of an

	electronic document is accurate? • How can the time of creation of an electronic record or the time at which it is sent or received be established with reasonable accuracy? • What electronic records management system can be used to ensure that electronic records are readily identifiable, retrievable and able to be read at a later date? • What electronic record retention policy should be adopted to ensure that any legal requirements for the preservation of records are met?

It is apparent that if the uncertainties associated with electronic contracting remain unresolved, then the practical consequences for contracting parties may be serious. On a more general level, these uncertainties will contribute to a reduced willingness by business to take advantage of modern communication technologies. As succinctly stated by Boss and Kaufman Winn (1997, p1470):

> The increased costs of dealing with these new legal uncertainties may offset any reduction in costs achieved through the use of new technologies and, as a result, may slow needlessly the rate at which businesses are willing to implement new technologies.

The remaining project deliverables for the CRC for Construction Innovation research project 2005-025-A *Electronic Contract Administration – Legal and Security Issues* will investigate possible solutions to the issues identified in this Report.

7. REFERENCES

Aalberts, B. & van der Hof, S., 2000, ‘Digital signature blindness: analysis of legislative approaches toward electronic authentication’, Number 32 in ITeR, Nationaal programma informatietechnologie en recht.pub-KLUWER. In English with summary in Dutch.

Adams, C., Chain, P., Pinkas, D. & Zuccherato, R., 2001, Internet {X.509} Public Key Infrastructure Time Stamp Protocol (TSP) Network Working Group, Standards Track, RFC 3161 available at http://www.ietf.org/rfc/rfc3161.txt (accessed 6 May 2006).

Ansper, A., Buldas, A., Saarepera, M. & Willemson, J., 2001, ‘Improving the Availability of Time-Stamping Services’, *Information Security and Privac’*, *6th Australasian Conference (ACISP)*, (V. Varadharajan, Y. M., ed) Lecture Notes in Computer Science pp. 360–375, Springer.

Argy, P., 2006, ‘Electronic Evidence, Document Retention and Privacy’, available at http://www.mallesons.com/search-hithighlight.cfm?hitURL=/publications/2006/Mar/8367966w.htm&keyword=electronic%20evidence (accessed 3 May 2006).

Argy, P. & Martin, N., 2001, ‘The Effective Formation of Contracts By Electronic Means’, *Computers & Law*, vol.46, p. 20, available at http://www.nswscl.org.au/journal/46/Argy.html (accessed on 5 June 2006).

Australian Law Reform Commission, 2005, *ALRC Discussion Paper 69 – Review of the Uniform Evidence Acts*, available at http://www.austlii.edu.au/au/other/alrc/publications/dp/69/ (accessed 1 March 2006).

Ballon, I.C., 1998, ‘How Companies Can Reduce the Costs and Risks Associated with Electronic Discovery’, *The Computer Lawyer*, vol.15, no. 7, p. 8.

Beale, H. & Griffiths, L., 2002, ‘Electronic Commerce: Formal Requirements in Commercial Transactions’, *Lloyd’s Maritime and Commercial Law Quarterly*, 2002, part 4, p. 467.

Becerik, B., 2004, *Critical Enhancements for Improving the Adoption of Online Project Management Technology*, Global Congress Proceedings – North America.

Bell, D. & LaPadula, L., 1973, *Secure Computer Systems: A Mathematical Model*, Technical Report MTR-2547, Vol. 2 MITRE Corp.

Bell, D. & LaPadula, L., 1975, *Secure Computer System Unified Exposition and Multics Interpretation*, Technical Report MTR-2997 MITRE Corp.

Bellare, M., Canetti, R. & Krawczyk, H., 1996, ‘Keying Hash Functions for Message Authentication’, *Advances in Cryptology - Crypto 96 Proceedings*, Lecture Notes in Computer Science Vol. 1109, N. Koblitz ed., Springer-Verlag, 1996. Full version of the paper is available at http://www-cse.ucsd.edu/users/mihir/papers/hmac.html (accessed 5 June 2006).

Bellare, M., Kilian, J. & Rogaway, P., 2000, ‘The security of the cipher block chaining message authentication code’, *Journal of Computer and Systems Science*, Vol. 61 (3), pp. 362–399.

Berning, P.W. & Diveley-Coyne, S., 2000, ‘E-Commerce and the Construction Industry: The Revolution Is Here’, available at http://www.constructionweblinks.com/Resources/Industry_Reports__Newsletters/Oct_2_2000/e-commerce.htm (accessed on15 December 2005).

Biba, K. J., 1977, *Integrity Considerations for Secure Computer Systems,* Technical Report MTR-3153, Rev. 1 MITRE Corp.

Black, J. & Rogaway, P., 2002, ‘A Block-Cipher Mode of Operation for Parallelizable Message Authentication’, *Advances in Cryptology – EUROCRYPT* 2002, International Conference on the Theory and Applications of Cryptographic Techniques, (Knudsen, L. R., ed), vol. 2332 *Lecture Notes in Computer Science*, pp. 384–397.

Boss, A.H. & Kaufman Winn, J., 1997, ‘The Emerging Law of Electronic Commerce’, *The Business Lawyer*, vol.52, p. 1469.

Brewer, D. F. C. & Nash, M. J.,1989, ‘The Chinese Wall Security Policy’ Proceedings of the 1989 *IEEE Computer Society Symposium on Security and Privacy* (SSP ’89), pp. 206–214.

Briggs I. & Brumpton, S., 2001, ‘Embrace E-Construction With Care!’, *Australian Construction Law Bulletin*, vol.13, no.4, p. 25.

British Institute of International and Comparative Law, 2006, *Digital Evidence Research Programme*, available at http://www.biicl.org/index.asp?contentid=1011 (accessed on 20 March 2003).

Buldas, A., Lipmaa, H. & Schoenmakers, B., 2000, ‘Optimally Efficient Accountable Time-Stamping’, *PKC: International Workshop on Practice and Theory in Public Key Cryptography*, (Imai, H. & Zheng, Y., eds) volume 1751 of *Lecture Notes in Computer Science* pp. 293–305.

Casamassima, T.J. & Caplicki, E.V., 2003, ‘Electronic Evidence at Trial: The Admissibility of Project Records, E-Mail and Internet Websites’, *The Construction Lawyer*, vol.23, no.3, p. 13.

Centre, C. S. S., 1993, *The Canadian Trusted Computer Product Evaluation Criteria,* Version 3.0e.

Chokhani, S. and Wallace, C., 2004, ‘Trusted Archiving’ Published at 3rd Annual *PKI R&D Workshop*, available at http://middleware.internet2.edu/pki04/proceedings/ (accessed 5 June 2006).

Christensen, S., 2001, ‘Formation of Contracts by Email – Is it Just the Same as the Post’, *Queensland University of Technology Law & Justice Journal*, vol.1, no. 1, p. 22

Christensen, S., Duncan, W. & Low, R., 2003, ‘The Statute of Frauds in the Digital Age – Maintaining the Integrity of Signatures’, *E Law – Murdoch University Electronic Journal of Law* vol.10, no. 4, available at http://www.murdoch.edu.au/elaw/issues/v10n4/christensen104.html (accessed 5 December 2005).

Christensen, S., Duncan, W. and Low, R., 2002. ‘Moving Queensland Property Transactions to the Digital Age: Can Writing and Signature Requirements be Fulfilled Electronically?’, available at http://www.law.qut.edu.au/files/digital.pdf (accessed 6 December 2005).

Clark, D. D. & Wilson, D. R.,1987, ‘A Comparison of Commercial and Military Computer Security Policies’, Proceedings of the 1987 *IEEE Symposium on Security and Privacy* (SSP ’87) pp. 184–195, IEEE Computer Society Press.

Commission of the European Communities (CEC), 1991, ITSEC, Information Technology Security Evaluation Criteria Version 1.2, June 1991.

Connolly, C. & Ravindra, P., 2005, ‘UN Releases New International Convention on Electronic Contracting’, *Internet Law Bulletin*, vol.7, no.10, p. 139.

Cryptomathic Time Stamping Authority (CTSA), 2003, *TSA Technical White Paper*, available at http://www.cryptomathic.com/pdf/ctsa_white%20paper.pdf (accessed 5 June 2006).

Daemen, J. & Rijmen, V., 2001, ‘Algorithm Alley: Rijndael: The Advanced Encryption Standard’, *Dr. Dobb’s Journal of Software Tools*, vol. 26 (3), pp. 137–139.

Davidson, A., 1999, 'Retaining electronic mail for evidentiary purposes', *Proctor*, vol.19, no. 6, p. 29.

Davidson, A., 2004, 'Signatures on Electronic Documents', *Proctor*, vol.24, no.7, p. 29.

De Zilva, A., 2003, 'Electronic Transactions Legislation: An Australian Perspective', *The International Lawyer*, vol.37, no.4, p.1009.

Defence Signals Directorate (DSD), 2006, *Australian Government Information Technology Security Manual* (ACSI 33), available at http://www.dsd.gov.au/library/infosec/acsi33.html. (accessed 2 June 2006).

Department of Justice: Canada, 2005, *A* Survey *of Legal Issues Relating to the Security of Electronic Information*', available at http://www.justice.gc.ca/en/ps/ec/toc.html (accessed 7 December 2005).

Department of Public Works and Services New South Wales, 2000, *Risk Management in Electronic Procurement*, available at http://www.cpsc.nsw.gov.au/e-procurement/docs/Risk-Chapter2.pdf (accessed 7 December 2005).

Diffie, W. & Hellman, M., 1976, 'New Directions in Cryptography', *IEEE Transactions on Information Theory*, vol. 22 (5), pp. 644–654, available at http://www-ee.stanford.edu/~hellman/publications.html (accessed 3 April 2006).

Digital Preservation Coalition, 2002, *Digital Preservation*, 15 December 2005, available at http://www.dpconline.org/graphics/digpres/presissues.html (accessed 5 June 2006).

Dumortier, J. & Van den Eynde, S., 2002, 'Electronic signatures and trusted archival services', Proceedings of the *DLMForum* 2002 pp. 520–524, Office for Official Publications of the European Communities, available at http://www.law.kuleuven.ac.be/icri/publications/172DLM2002.pdf?where=. (accessed 7 April 2006).

Edwards, L. & Waelde, C., (eds), 1997, *Law and the Internet: Regulating Cyberspace*, Hart Publishing, Oxford.

Electronic Commerce Expert Group of the Attorney General, 1998, 'Electronic Commerce: Building the Legal Framework', available at http://web.archive.org/web/20021015155004/http://law.gov.au/aghome/advisory/eceg/ecegreport.html (accessed 8 May 2006).

Federal Information Processing Standards (FIPS) 180-2, 2002, 'Secure Hash Standard'' *National Institute of Standards and Technology (NIST*), available at http://csrc.nist.gov/publications/fips/fips180-2/fips180-2.pdf (accessed 5 June 2006).

Ferraiolo, D. F., Kuhn, D. R. & Chandramouli, R., 2003,. *Role-Based Access Control,* Artech House.

Forbes, J.R.S., 2004, *Evidence Law in Queensland* (5th ed), Thomson, Sydney.

Freier, A. O., Karlton, P. & Kocher, P. C., 1996, *The SSL Protocol - Version 3.0 Internet Draft*, Transport Layer Security Working Group.

Gauravaram, P., McCullagh, A. & Dawson, E., 2006, 'Collision Attacks on MD5 and SHA-1: Is this the "Sword of Damocles for Electronic Commerce?' To appear in the proceedings of *AusCert* 2006, available at http://www.isi.qut.edu.au/people/subramap/. (accessed 4 April 2006).

Geiger, D.R., 1999, 'Failure to Preserve Email and Discovery', *Internet Law Bulletin*, vol.2, no.6, p. 81.

Giles, D., 2000, 'You've Got Mail…Or Have You?', *Internet Law Bulletin*, vol.3, no.1, p. 12.

Givens, J.S., 2003/2004, 'The Admissibility of Electronic Evidence At Trial: Courtroom Admissibility Standards', Cumberland Law Review, vol.34, no1, p. 95.

Gollmann, D.,1999, *Computer Security*, John Wiley & Sons, New York.

Goodwin, R., Goh, S. & Wu, F., 2002, 'Instance-level access control for business-to-business electronic commerce', *IBM Systems Journal*, vol. 41 (2), pp. 303.

Gorry, S., 1997, 'Electronic Records and the Evidence Act', *Australian Company Secretary*, vol.49, no.2, p. 60.

Haber, S. & Stornetta, W. S., 1991, 'How to Time-Stamp a Digital Document', *Journal of Cryptology*, 3 (2), 99–111.

Halsbury, H.S.G.,1991, *Halsbury's Laws of Australia*, Butterworths, Sydney.

Hill, S.W.B., 2001, 'Email Contracts – When is the Contract Formed?', *Journal of Law and Information Science*, vol.12, no.1, p. 46.

Hill, S.W.B., 2001, 'Flogging A Dead Horse – The Postal Acceptance Rule and Email', *Journal of Contract Law*, vol.17, no.2, p. 151.

Hill, S.W.B., 2002, 'Formation of Contracts Via Email – When and Where?', *Commercial Law Quarterly*, vol.16, no.1, p. 3.

Hogan-Doran, J., 2003, 'Jurisdiction in Cyberspace: The When and Where of On-line Contracts', *Australian Law Journal*, vol.77, no.6, p. 377.

Howie, J., 2005, 'Deleting E-mail Could Result in Huge Liability', *Contract Management*, vol.45, p. 4.

Huey, N.A., 2003, 'E-mail and Iowa's Statute of Frauds: Do E-Sign and UETA Really Matter?', *Iowa Law Review*, vol.88, no.3, p. 681.

Hultmark Ramberg, C., 2001, 'The E-Commerce Directive and Formation of Contract in a Comparative Perspective', *Global Jurist Advances*, vol.1, no.2, p. 1.

International Chamber of Commerce, 2001, *GUIDEC II – General Usage for International Digitally Ensured Commerce*, available at http://www.iccwbo.org/home/guidec/guidec_two/contents.asp (accessed 5 December 2005).

International Chamber of Commerce, 2004, *ICC eTerms*, available at http://www.iccwbo.org/policy/law/id279/index.html (accessed 5 December 2005).

International Standards Organisation, International Electrotechnical Commission (ISO 1999), Standard ISO/IEC 15408: Evaluation criteria for information technology, 1999.

Iwata, T. & Kurosawa, K., 2003, 'OMAC: One-Key CBC-MAC', *Fast Software Encryption*, 10th International Workshop, FSE 2003, Lund, Sweden, February 24-26, 2003, Revised Papers, (Johansson, T., ed) volume 2887 of *Lecture Notes in Computer Science* pp. 129–153, Springer.

Just, M., 1998a,. *On the Temporal Authentication of Digital Data*, PhD Thesis, Carleton University.

Just, M., 1998b, 'Some Timestamping Protocol Failures', Proceedings of the *Symposium on Network and Distributed Systems Security* (NDSS '98), Internet Society, available at http://www.isoc.org/isoc/conferences/ndss/98/just.pdf (accessed 6 April 2006).

Kamara, J. & Pan, D.Y.H., 2004, 'Virtual Collaborative Design', *Construction Information Quarterly*, vol 6, no 2, p. 170.

Kidd, D.L. & Daughtrey Jnr, W.H., 2000, 'Adapting Contract Law to Accommodate Electronic Contracts: Overview and Suggestions', *Rutgers Computer & Technology Law Journal*, vol.26, no.2, p. 215.

Laryea, E. T., 1999, 'The Evidential Status of Electronic Data', *National Law Review,* Issue 3, p. 6.

Lawrence, A., 2000, 'Fundamental Issues For Electronic Transactions: the Value of Authentication', *Internet Law Bulletin*, vol.3, no.6, p. 85.

Ligertwood, A., 2004, *Australian Evidence*, LexisNexis Butterworths, Australia.

Lim, Y.F., 2002, *Cyberspace Law: Commentaries and Materials*, Oxford University Press, Melbourne.

Lynch, C., 2004, ‘Preserving Digital Documents: Choices, *Approaches and Standards’ Law Library Journal*, vol.96, no.4, p. 609.

Mallesons, 2003, ‘Email and Contractual Notices’, available at http://www.mallesons.com/search-hithighlight.cfm?hitURL=/publications/Asian_Projects_and_Construction_Update/6497970W.htm&keyword=electronic%20transactions%20act (accessed 4 May 2006).

Mason, S., 2002a, ‘The Evidential Issues Relating to Electronic Signatures – Part I’, *Computer Law & Security Report*, vol.18, no.3, p. 175.

Mason, S., 2002b, ‘The Evidential Issues Relating to Electronic Signatures – Part II’, *Computer Law & Security Report*, vol.18, no.4, p. 241.

McCullagh, A., Caelli, W. & Little, P., 2001, ‘Signature Stripping: A Digital Dilemma', *The Journal of Information, Law and Technology,* Issue No1, available at http://www2.warwick.ac.uk/fac/soc/law/elj/jilt/2001_1/mccullagh/ (accessed 5 June 2006).

Mills, D., 2006, ‘Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI’, Internet informational RFC 4330, available at http://www.rfc-archive.org/getrfc.php?rfc=4330 (accessed 6 May 2006).

Mills, D. L., 1992, ‘Network Time Protocol (Version 3) --- Specification, Implementation and Analysis’, Internet draft standard RFC 1305, available at http://www.ietf.org/rfc/rfc1305.txt (accessed: 5 April 2006).

Mills, D. L., 1996, ‘Simple Network Time Protocol (NTP) Version 4 for IPv4, IPv6 and OSI’, Internet informational RFC 2030, available at http://www.rfc-archive.org/getrfc.php?rfc=2030 (accessed: 5 April 2006).

Naismith, P.G., 2003, ‘The Discovery of Electronic Evidence’, *Journal of Judicial Administration*, vol.12, no.4, p. 180.

National Archives of Australia, 2004, *Digital Recordkeeping – Guidelines for Creating, Managing and Preserving Digital Records (Exposure Draft May 2004)*, available at http://www.naa.gov.au/recordkeeping/er/guidelines/DigitalRecordkeeping.pdf (accessed 19 December 2005).

National Bureau of Standards (NBS), 1977, *Federal Information Processing Standards Publication* (FIPS PUB) 46.

National Institute of Standards and Technology (NIST), 1995, ‘An Introduction to Computer Security: The NIST Handbook’, special publication 5, Number SP 800-12, available at http://csrc.nist.gov/publications/nistpubs/800-12/handbook.pdf (accessed 6 May 2006).

National Institute of Standards and Technology (NIST), 1999, ‘Data Encryption Standard (DES)’, FIPS Publication 46-3, available at http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf (accessed 8 April 2006).

National Institute of Standards and Technology (NIST), 2000, ‘Federal Information Processing Standards (FIPS) PUB 186-2’, Digital Signature Standard (DSS), available at http://csrc.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf (accessed 3 April 2006).

National Institute of Standards and Technology (NIST), 2001, ‘Advanced Encryption Standard’, available at http://csrc.nist.gov/CryptoToolkit/aes/ (accessed 5 April 2006).

National Institute of Standards and Technology (NIST), 2005, ‘Brief Comments on Recent Cryptanalytic Attacks on SHA-1’, available at http://csrc.nist.gov/news-highlights/NIST-Brief-Comments-on-SHA1-attack.pdf (accessed 5 June 2006).

National Office for the Information Economy, 2002, *National Electronic Authentication Council Report on Liability and Other Legal Issues in the Use of PKI Digital Certificates*.

Nicoll, C., 2000, 'Consent – The Luddite's Lifeline', *Information & Communications Technology Law*, vol.9, no.3, p. 195.

Nikolich, M., 2003, 'The Legality of E-mail Messages', *Australian Construction Law Newsletter*, vol.91, p. 27.

Ogders, S., 2000, *Uniform Evidence Law* (4th ed), LBC Information Services, Australia.

O'Shea, K. & Skeahan, K., 1997, 'Acceptance of Offers by E-Mail – How Far Should the Postal Acceptance Rule Extend?', *Queensland University of Technology Law Journal*, vol.13, p. 247.

Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy, 2005, *The Use of Authentication Across Borders in OECD Countries*, available at http://www.oecd.org/dataoecd/1/10/35809749.pdf (accessed 5 December 2005).

Pfleeger, C. P.,1997, *Security in Computing*, Designing Trusted, Prentice-Hall International.

Pitiyasak, S., 2003, 'Electronic Contracts: Contract Law of Thailand, England and UNCITRAL Compared', *Computer and Telecommunications Law Review*, vol.9, p. 16.

Queensland Government, 2003, *Best Practice Guide to Recordkeeping*.

Reed, C., 2001, 'Legally Binding Electronic Documents: Digital Signatures and Authentication', The International Lawyer, vol.35, no.1, p. 89.

Reynolds, P., 1994, Admissibility of computer-produced documents as evidence, *Computer Law and Practice,* Volume 10, p. 118.

Robins, M.D., 2003, 'Evidence at the Electronic Frontier: Introducing Email at Trial in Commercial Litigation', vol.29, no.2, p. 219.

RSA Laboratories, 2002, 'PKCS #1 v2.1: RSA Cryptography Standard', RSA Data Security, Inc., available at http://www.rsasecurity.com/rsalabs/node.asp?id=2125 (accessed 8 April 2006).

Security Technology Competence Centre (SETCCE), 2005, *Trusted Electronic Archive White Paper*, available at http://www.setcce.si/eng/download/Trusted_Electronic_Archives_-_White_Paper.pdf (accessed 5 June 2006).

Seddon, N.C. & Ellinghaus, M.P. (eds), 2002, *Cheshire & Fifoot's Law of Contract*, 8th ed, LexisNexis Butterworths, Chatswood.

Sheridan, N. & Rigotti, M., 2001, 'Contract Formation and Electronic Signatures Under the Electronic Transactions Act', *Journal of Banking and Finance Law and Practice*, vol.12, no.1, p. 47.

Shrivastava, S., 2004, *Security and Trust in Composite Services*, available at http://adapt.ls.fi.upm.es/deliverables/d12.pdf (accessed 2 May 2006).

Sneddon, M., 2000, 'Legal Liability and e-transactions' (A scoping Study for the National Electronic Authentication Council)', available at http://unpan1.un.org/intradoc/groups/public/documents/APCITY/UNPAN014676.pdf (accessed 5 December 2005).

Spenceley, C., 2003, 'Evidentiary Treatment of Computer-Produced Material: A Reliability Based Evaluation', *Thesis*, University of Sydney.

Standards Australia, 2003, *Guidelines for the Management of IT Evidence*, HB 171-2003, Sydney, 15 December 2005.

Stanfield, A., 2005, 'Electronic discovery – what are your duties?' Australian Law Management Law Journal, Winter 2005, p. 12.

Stim, R., 2004,. *License Your Invention: Sell Your Idea and Protect Your Rights with a Solid Contract,* Nolo Press.

Taylor, C., 2005, 'Web-based collaboration tools for the construction industry: the John Holland Experience', CRC CI International Conference, 25-27 October 2004, Surfers Paradise, Australia Proceedings of Clients Driving Innovation International Conference 2004.

Thompson, J., 2003, 'Has the New State Electronic Transactions Act Solved All Our Problems?', *Brief*, vol.20, no.11, 26.

Thompson, S., 2004, 'E-commerce, E-Security and Contracting', *Australian Business Law Review*, vol.32, no.2, p.132.

Tuma. S.E. & Ward, C.R., 2000, 'Contracting Over the Internet in Texas', *Baylor Law Review*, vol.52, no.2, p. 381.

United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP), 2005, *E-Commerce Legal Issues*, available at http://unescap.org/tid/gateway/tisgway%5Fecom.pdf (accessed 5 December 2005).

United Nations Economic Commission for Europe (UNECE), 2000, *Recommendation 31 Electronic Commerce Agreement (ECE/TRADE/257)*, available at http://www.unece.org/cefact/recommendations/rec31/rec31_ecetrd257e.pdf (accessed 20 March 2006).

United Nations, 2005, *Convention on the Use of Electronic Communications in International Contracts*, available at http://www.uncitral.org/pdf/english/texts/electcom/ch_X_18.pdf (accessed 21 March 2006).

Verisign, 1998, *About Digital IDs*, available at http://www.adobe.com/security/digsig.html (accessed 30 April 2006).

Walsh, N., 1998, *A Technical Introduction to XML*, available at http://www.xml.com/pub/a/98/10/guide0.html (accessed 10 May 2006).

Walters, M.D. & Wright, N., 2005, 'Electronic Evidence Update: How to Help Clients Meet Their Duty to Preserve Evidence in the Computer Age', Washington State Bar News, vol.59, no.7, p. 16.

Wang, X. & Yu, H., 2005, 'How to Break MD5 and Other Hash Functions' *Advances in Cryptology - EUROCRYPT2005,* Cramer, R., ed., volume 3494, *Lecture Notes in Computer Science* pp. 19–35, Springer.

Wang, X., Feng, D., Lai, X. & Yu, H., 2004, 'Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD' *Cryptology* ePrint Archive, Report 2004/199, available at http://eprint.iacr.org/ (accessed 5 June 2006).

Wang, X., Lai, X., Feng, D., Chen, H. & Yu, X., 2005a, 'Cryptanalysis of the Hash Functions MD4 and RIPEMD', *Advances in Cryptology - EUROCRYPT 2005*, Cramer, R., ed., volume 3494 of *Lecture Notes in Computer Science*, pp. 1–18, Springer.

Wang, X., Yin, Y. L. & Yu, H., 2005b, 'Finding Collisions in the Full SHA-1', *Advances in Cryptology—CRYPTO '05*, (Shoup, V., ed) volume 3621 of Lecture Notes in Computer Science pp. 17–36, Springer, 2005.

Wang, X., Yin, Y. L. & Yu, H., 2005c, Efficient Collision Search Attacks on SHA-0', *Advances in Cryptology—CRYPTO '05*, Shoup, V., ed., volume 3621 of *Lecture Notes in Computer Science* pp. 1–16, Springer, 2005.

Webopedia, 2006. The definition is available at http://www.webopedia.com/TERM/E/errordetection.html (accessed 10 April 2006).

White, S., 2001, 'Discovery of Electronic Documents', *Computers & Law*, vol.44, p. 46.

Wilkinson, P., 2005, *Construction Collaboration Technologies: The Extranet Revolution*, Taylor & Francis, London; New York.

Williams, N., 2005, *Outsourcing Considerations for Electronic Records Archiving*, available at http://www.ecominfo.net/arts/777_legato_outsourcing.htm (accessed 6 December 2005).

Willmott, L. Christensen, S. and Butler, D. 2005, *Contract Law*, Oxford University Press, Melbourne, Australia.

Wolfson, A., 2005, '"Electronic Fingerprints": Doing Away with the Conception of Computer-Generated Records as Hearsay', *Michigan Law Review*, vol.104, no.1, p. 151.

Xiaoyun Wang, A. Y. & Yao, F., 2005, 'New Collision Search for SHA-1', Presented at Crypto'05 Rump Session by Adi Shamir. There is no official paper yet that explains this new result.

8. AUTHOR BIOGRAPHIES

Professor Ed Dawson
Information Security Research Centre
Faculty of Information Technology
Queensland University of Technology
Ph +61 7 3864 9551, Fax +61 7 3864 1801, email e.dawson@qut.edu.au

Professor Dawson is the Director of the Information Security Research Centre. He has research experience in many aspects of cryptology. He has published over 200 research papers in various aspects of cryptology. He has extensive research experience in the applications of cryptology, especially to e-commerce.

Professor Sharon Christensen, LL.B.(Hons)(QIT), LL.M.(QUT), Solicitor, Queensland
School of Law
Queensland University of Technology
Ph +61 7 3864 5204, fax +61 7 3864 2121, email s.christensen@qut.edu.au

Professor Christensen is the Gadens Professor in Property Law at the Queensland University of Technology. She has written and lectured in Land Contracts and Contract and has research interests in contract, property law and electronic transactions. She is a specialist consultant at Gadens Lawyers, Brisbane and a Deputy Director of the Information Security Institute.

Professor William Duncan, LL.B.(Qld), LL.M.(Lond.), Solicitor, Queensland
School of Law
Queensland University of Technology
Ph +61 7 3864 2709, fax +61 7 3864 1161, email w.duncan@qut.edu.au

Professor Duncan is a Professor of Law at the Queensland University of Technology and consultant to Allens Arthur Robinson, Brisbane. He has written and lectured extensively in the subjects of property law, land contracts and allied subjects in tertiary institutions in Queensland and to the legal profession since 1973.

Ms Kathryn O'Shea LL.B.(Hons)(QUT), Solicitor, Queensland
School of Law
Queensland University of Technology
Ph +61 7 3864 5207, fax +61 7 3864 2121, email k.oshea@qut.edu.au

Ms O'Shea is an Associate Lecturer in the School of Law of the Queensland University of Technology. Prior to joining the university in 2005, she worked for an extensive period of time as a solicitor in private practice in the corporate and commercial areas. She has practised in national and international firms in both Brisbane and London. Her current research interests include electronic transactions, contract law and consumer protection.

Ms Judith McNamara LL.B (Hons)(Qld)**,** LLM(QUT), Solicitor, Queensland
School of Law
Queensland University of Technology
Ph +61 7 3864 5212, fax +61 7 3864 2121, email j2.mcnamara@qut.edu.au

Ms McNamara is an Associate Lecturer in the School of Law of the Queensland University of Technology. Prior to joining the university in 2006, she was an Associate Lecturer at the University of Southern Queensland and has worked as a solicitor in private practice. Her current research interests include electronic commerce law, intellectual property and privacy.

Dr Ernest Foo, B.E. (Hons)(UQ), PhD(QUT).
Information Security Research Centre
Faculty of Information Technology
Queensland University of Technology
Ph +61 7 3864 9554, Fax +61 7 3864 1801, email e.foo@qut.edu.au

Dr Foo is a Lecturer in the Faculty of Information Technology at the Queensland University of Technology. He is also an active researcher in the Information Security Research Centre. Dr Foo has research interests in the field of electronic commerce, in particular the development of secure protocols.

Dr Audun Josang
School of Software Engineering and Data Communications
Faculty of Information Technology
Queensland University of Technology
Ph +61 7 3864 2960, Fax +61 7 3864 1214, email a.josang@qut.edu.au

Associate Professor Audun Josang joined QUT in August 2005. Prior to that, he was the research leader of the Security Unit at DSTC in Brisbane, worked in the telecommunications industry for Alcatel in Belgium and for Telenor in Norway. He was also Associate Professor at the Norwegian University of Science and Technology (NTNU). He has a Masters degree in Information Security from Royal Holloway College at the University of London, and a PhD from NTNU in Norway. Prof. Josang has more than 60 scholarly publications, and his research focuses on security and trust management.

Mr Praveen Guaravaram, B.Tech (EEE, S.VU.C.E, India), MIT (QUT)
Information Security Institute
Faculty of Information Technology
Queensland University of Technology
Ph +61 7 3864 9557, Fax +61 7 3221 2384 email p.gauravaram@isi.qut.edu.au

Mr Gauravaram is a research associate in the Information Security Institute (ISI), QUT and is presently undertaking a PhD in the area of analysis, design and applications of cryptographic hash functions. He is also a tutor in the Faculty of Information Technology (FIT), QUT. His current research interests include the analysis and design of cryptographic primitives, applied cryptography and information security.