Papua New Guinea

CONSTITUTIONAL & LAW REFORM COMMISSION

Review of Proof of Business and Electronic Records

FINAL REPORT

FINAL REPORT 4
February 2012

Published in Port Moresby by:

Constitutional and Law Reform Commission
Level 2, First Heritage Centre, Hohola
National Capital District

Telephone: (675) 325 2862
(675) 325 2840

Website: www.clrc.gov.pg
Fax: (675) 325 3375
Email: ericlkwa@gmail.com
clrcpng@gmail.com

ISBN: 9980-9900-8-2

Terms of Reference

CLRC Reference No 4: Proof of Business & Electronic Records.

I, Bire Kimisopa, Minister for Justice, by virtue of the power conferred on me by Section 12 of the *Constitutional and Law Reform Commission Act* 2004 (the Act) refer and direct as follows.

(1) I refer to the Constitutional and Law Reform Commission (the Commission) for enquiry and report on their systematic development and reform, in accordance with s. 12 of the Act whether and how the laws of evidence can or should be modified to permit the proof of:

- (a) business records; and
- (b) electronic records and electronic communications (email); and
- (c) to the extent necessary to achieve the reforms proposed in relation to (a) and (b), whether and how any relevant associated laws and practices should also be modified.

(2) I direct that in undertaking the investigation and report, the Commission shall:

- (a) consider any relevant research or developments, whether in this or other jurisdictions on the matter for inquiry; and
- (b) consult widely within the community, particularly the business community, and the legal profession, and also within the Government, particularly the courts, the Ombudsman Commission and the Department of Justice and Attorney General.

(3) The Commission shall report to me within 8 months of the date of publication of this reference in the Government Gazette.

(4) This reference shall be referred to as: *CLRC Reference No 4: Proof of Business & Electronic Records.*

Dated this ***2nd*** day of ***November*** 2006**.**

Hon Bire Kimisopa, MP
Minister for Justice

Participants

The Commissioners of the Constitutional and Law Reform Commission (CLRC) are:

- Hon. Joe Mek Teine MP — Chairman
- Mr. Gerhard Linge, — Deputy Chairman
- Prof. Betty Lovai
- Mr. Tom Anayabere
- Hon. Malakai Tabar MP
- Hon. Puri Ruing MP
- Professor John Luluaki

The Commissioners appointed Hon. Joe Mek Teine LLB MP to supervise this reference. The CLRC then established a Working Committee comprising representatives from key organizations to guide and supervise the work in this reference on Business and Electronic Records. The Working Committee comprised:

- Mr. Vergil Narakobi, Law Society Nominee , Narakobi Lawyers - Chairman
- Mr. Molean Kilepak, Executive Branch, Department of Justice & Attorney General
- Mr. Alex Tongayu, Deputy Registrar of Companies, IPA & Securities Commission of PNG
- Ms. Amanda Nambau, Lawyer, Posman Kua Aisi Lawyers
- Mr. Ronald Maru, First Assistant Secretary (Policy Planning & Information) Department of Commerce & Industry
- Mr. Anthony Nakuk, Assistant Secretary (Planning, Statistics & Information), Department of Commerce & Industry
- Mr. Ravu Auka, Deputy Public Prosecutor (Courts)
- Mr. Nick Mosoro, Lawyer, Executive Branch, Department of Justice & Attorney General
- Mr. Vincent Bull, Local Managing Partner, Allen Arthur Robinson Lawyers
- Mr. Oakaiva Oiveka, Lawyer, Public Solicitor

Contents

1. Introduction to the Inquiry

Contents

1.1 The Constitutional and Law Reform Commission

The Constitutional and Law Reform Commission (CLRC) is an amalgam of the former Constitutional Development Commission (CDC) and the Law Reform Commission (LRC). It was established on 4th March, 2005 under the *Constitutional and Law Reform Commission Act* 2004. As stipulated under Section 12 of its Act, the CLRC:

- receives a reference from the Minister for Justice to conduct its review and propose legislative changes where appropriate concerning laws other than constitutional laws; or
- receives a reference from the Head of State acting on advice from the executive government to conduct its enquiry and review into any parts of the Constitution and the Organic Laws and propose appropriate constitutional reform where considered appropriate.

1.2 Objectives of this Reference: CLRC Reference No. 4: Proof of Business & Electronic Records

The primary objective of this Reference is to inquire into and review the laws of evidence so as to assess and determine:

- whether and how the laws of evidence can or should be modified to permit the proof of business records; in the form of electronic records and electronic communications (email),
- if the laws of evidence are to be modified, what should be done and how best should that be achieved?;

- if the laws of evidence are to be amended, then propose and recommend appropriate legislative amendments to relevant legislation or even the new provisions or if not, propose and recommend the enactment of new legislation, and
- to the extent necessary to achieve the reforms proposed above, whether and how any relevant associated laws and practices should also be modified .

1.3 Purpose and Scope of this Reference

The purpose and scope of this Reference is as stated in the Reference itself – being to review and propose how best the laws of evidence can or should be modified to allow for the proof of:

- business records;
- electronic records and electronic communications (email), and
- to give effect to any of the above, propose and recommend further reforms to related or associated laws.

In particular, the scope of this Reference is to:

- review the relevant provisions of the *Evidence Act* Chapter 48 and related legislation and to allow for the proof of business records, electronically generated communication including emails, and
- identify any gaps, if any, in the current laws and to recommend appropriate reform measures to fill those gaps particularly relating to the proof of electronic records and electronic communications (email).

It may be a much longer bow to attempt to include in this Reference the crimes committed on the internet (cyber crime) such as tampering with another person's computer and obtaining information from it; interfering with another's computer data or computer system; trafficking in illegal computer devices; various fraudulent activities on the internet;[1] etc. It is our view that since these are crimes, such should be dealt with separately by a review of the relevant parts of the *Criminal Code* or such other crimes

[1] Such was undertaken by the Kingdom of Tonga under the *Computer Crimes Act* 2003 discussed in Blythe S. "South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga" (2006) 10(1) *Journal of South Pacific Law* http://www.paclii.org/journals FJAPL/vol 10/2.shtml viewed on 8 September 2008

legislation. We should not venture into this area of the law, It is outside the scope of this Reference.

1.4 Consultations

For purposes of achieving the above objectives, the CLRC was directed to consult widely within the country, particularly in the business community, in the legal profession, and also within the Government, particularly the courts, the Ombudsman Commission and the Department of Justice and Attorney General. Outside of the country, we have been directed to consider any relevant research or developments of comparative value to this inquiry.

For purposes of identifying the issues and producing this Draft Report, the CLRC conducted initial consultations within the National Capital District with relevant stakeholders. Those consulted were Global Internet Ltd, Masalai Communications, Interpol, National Intelligence Organization, Post PNG Ltd, Port Moresby General Hospital, Steamships Ltd, City Pharmacy Ltd (CPL), Bank South Pacific, UPNG Law School, National Research Institute, National Statistics Office, National Executive Council and Westpac Bank.

The CLRC has considered all matters arising in response to the Issues Paper and is now able to release this Draft Report for further discussion. The CLRC invites further comments and submissions based on the proposals made in the Draft Report and will then proceed to issue its final report on the CLRC Reference No. 4.

Our timetable for the conduct of this review is as follows:

Deliverables	**Deadlines**
Release of Issues Paper	Friday, 26th June, 2009
Release of Draft Report	Wednesday, 29th February, 2012
Presentation of Report to Minister	Friday, 4th May, 2012

1.5 Purposes of this Draft Report

The primary purpose of this Draft Report is to provide background information and context on the subject matter of the Reference and then to focus and state the issues which, at the outset were envisaged. As indicated above, the Draft Report also states the time frame for this review and invites submissions on proposals contained in this Report. This Draft Report reflects the views of the stakeholders and the general public, and highlights the assessment and conclusions of the CLRC.

1.6 Structure of this Report

This paper is structured as follows:

- Chapter 2 provides a brief outline on the nature of the Proof of Business and Electronic Records.
- Chapter 3 provides an overview of existing law on the Reference;
- Chapter 4 presents and analyses the comparative material concerning the utilization and regulation of electronic transactions and electronic records;
- Chapter 5 presents the main proposals for consideration .

Contents

2.1 Introduction

In this part we begin by introducing and stating what "business records", "electronic records" and "electronic communications are. We then attempt to explain their nature for the purpose of this Paper..

We hope that the public is then better informed to make relevant input, comments, and suggestions on the proposals presented in this Report.

2.2 What are "Business Records", "Electronic Records", and "Electronic Communication"

(a) Business Records

The current *Evidence Act* does not have a definition of the term "Business Record", but does contain a definition of 'businesses'. According to the *Evidence Act*, "business" is the word defined broadly to include public administration and a business, profession, occupation, trade, undertaking, or calling of any kind.[2] From this definition it can be inferred that "Business Records" for the purposes of the *Evidence Act* may refer to any records concerning the conduct of public administration, the conduct of business in commerce and trade, or the conduct of business in any profession, occupation, trade or any calling. In other words, we can say that business records are records, which are created in the conduct of business and

[2] S1, *Evidence Act*, Chapter 48

communicated between parties to that business.[3] The following are typical examples of business records: books of account, accounting records of all kinds, employment records, production, job and work records of all kinds, stock records, dispatch, delivery or receipt of goods records, postage books, surveyors' field books, transport drivers' logs, hospital records, medical records of a doctor in private practice, inter-office memoranda, office diaries, and files of correspondence.[4]

(b) Electronic Records and Electronic Communications

Owing to its time, the *Evidence Act* does not specifically define "electronic records". For our purposes we adopt the following definition: as records created in the conduct of business and communicated between parties to that business through any medium of electronic communication. It has been suggested by some archivists that records must be set aside in the course of business to be considered as "record". Others argue that, the fact of being transacted in a particular business context is crucial to record, thus an adequate record will contain evidence of the context of its creation. As such electronic records are evidence of transactions (relationships of acts), means of action, and information about acts.

What is electronic communication?

There are a number of sources we have consulted for a working definition for our purpose. For instance, the Commonwealth of Australia *Electronic Transaction Act* 1999 offers the following definition for the term "electronic communication":

> (a) a communication of information in the form of data, text or images by means of guided and/or unguided electromagnetic energy; or
>
> (b) a communication of information in the form of speech by means of guided and/or unguided electromagnetic energy, where the speech is processed at its destination by an automated voice recognition system.[5]

Email means electronic mail; a data message (information generated, sent, received, or stored by electronic, optical or similar means including, but not

---

[3] Note 2, supra

[4] Meares C.L.D. & T.W.Waddell, "Report 17 (1973) – Evidence (Business Records)" (1973) http://www.lawlink.nsw.gov.au/lrc.nsf/pagesr17toc at April 14, 2008.

[5] *Australian Electronic Transactions Act* 1999

limited to, electronic data interchange, electronic mail, telegram, telex or telecopy, used or intended to be used as a mail message between the originator and addressee in an electronic communication.[6]

In our view, the above definition is very technical and complicated to some of our readers. We therefore prefer the approach taken and definition adopted by the United Nations Commission on International Trade Law (UNICTRAL), Working Group IV (Electronic Commerce)[7] where it first defined electronic communication to mean "any communication that the parties make by means of data messages." It defined data message as:

> "information generated, sent, received or stored by electronic, optical or similar means including, but not limited to electronic data interchange (EDI), electronic mail, telegram, telex or telecopy."

2.3 Background to this Reference

The unprecedented technological advances made in Information Technology (IT) – in particular the evolution of the internet and the World Wide Web (w.w.w.) has brought new challenges as well as opportunities to everyone in the world, including the people of Papua New Guinea. In this Reference our focus is more on the challenges rather than on the opportunities. The challenges are in the area of the law of evidence and the law of contract in dealing with these advancements, which have left the law somewhat stranded.

Never like before, an ever increasing number of Papua New Guineans – from private citizens to business houses, professional men and women to primary school pupils and of course the Government institutions - are now accessing information and communicating through the internet. The electronic mail (email) is now one of the most convenient, flexible, and accepted popular mode of communication and conducting business, irrespective of distance and difference in time zones of the global world. Simply through the click of a mouse or a button, communication(s) and transaction(s) are effected instantly.

The challenge for the law of evidence that we are focusing on in this Reference arises because the current *Evidence Act* was enacted back in 1975 or even back still. The internet and World Wide Web were never

---

[6] *Australian Electronic Communications and Transactions Act* 2002

[7] Fourty-fourth Session Vienna 11-22 October, 2004.

around. Neither the common law of England, which now applies in PNG as part of the underlying law, is of much assistance owing to the same reasons.

Most countries in the region and the world have made necessary legislative changes to address the challenges brought about by the internet and the World Wide Web. For example, in 1999 the Commonwealth of Australia enacted *Electronic Transaction Act* and the Republic of Vanuatu moved in 2000 to enact its *Electronic Transaction Act*.

The United Nations, through the United Nations Commission on International Trade Law (UNCITRAL) realising the importance of this matter, issued the *Model Law on Electronic Commerce* and the *Model Law on Electronic* Signatures in 1996 in an attempt to create a uniform global legal response to developments in the electronic media. A number of countries including Singapore, Canada, and Australia have embraced the general framework of these Model Laws to legislate in this area. These model laws attempt to provide national legislative guidelines of some internationally acceptable rules with the aim of creating a more secure legal environment and removing obstacles for electronic commerce, both nationally and globally.

2.4 Business Records, Electronic Records and the Law

Business records, electronic records, and electronic communication (email) are the means of communication in electronic commerce. They are important in the modern society because considerable use is made of electronic communication by government and businesses for keeping and producing records. An increasing number of transactions in international trade in PNG are carried out by means of communication known as electronic communications. It involves the use of alternatives to paper-based forms of communication, storage, and authentication of information. The Model Law on Electronic Commerce that UNCITRAL developed adopts a technology neutral approach. The Model Law was conceived to further the progressive harmonization and unification of the law of international trade. The Model Law respects the interests of all peoples, particularly those of developing countries.[8]

The General Assembly recommended that all States should give favourable consideration to the Model Law when enacting or revising their laws so that the legislation avoids preferring one form of electronic technology over any

[8] Attorney General Department, "UNCITRAL Working Group on Electronic Commerce" (2005) http://www.ag.gov.au/www/agd/agd.nsf/Page/e-commerce at 15 April 2008._

other. It must treat electronic transactions in the same way as paper based transactions.[9]

Generally the ability of the current law of evidence to deal with business and electronic records is very limited. There are no separate provisions, which allow for the proof of business records in electronic form. There are, however, provisions that deal with computerized information or those that allow for the proof of statements in documents produced by computers.[10] However, there are limitations. Documents that a computer produces may be admissible, but inadmissible if such were produced by other related means, such as electronic transactions using smart phones, flash drives CDs, DVDs, internet, emails, mobile phones, digital cameras, ipod, MP3s or telephone voicemails. To permit the proof of business and electronic records in the laws of evidence, consideration must be given to the modern information and communication technology. Electronic commerce and electronic signatures which business and electronic records are a part of this consideration.

In fairness, we point out that the *Evidence Act* was enacted in the 1970s. It ignores much of what is happening now, considering the development of modern information and communication technology and the effect of such modern information. Proof of technology requires the need to develop or revise the existing legislation that must ensure that records kept /produced/accessed electronically through any form of modern devices that can be admissible in the court of law. The challenge presented by computer databases is to determine whether free excess to the internet will make freedom of information legislation meaningless, unless we have legislation that regulates access, production, and the misuse of personal information in databases.

2.5 The Nature of Electronic Commerce

The advent of the internet and the World Wide Web saw an increase in the volume of electronic commerce. Electronic commerce is, of course, generated through electronic communication, largely through electronic mail (email) and accessing information and related material posted on the various websites. This type of activity is also known as electronic commerce (e-commerce). In very simple terms, e-commerce is the process of doing business on the internet electronically where transaction(s) may include consumer and business do business transactions where necessary

[9] Ibid
[10] *Evidence Act* 1975 Chapter 48 s 64 - 67

information to effect and conclude the business transaction are conducted or transacted. This may include online credit card transactions, electronic invoices, purchase order, and even e-billing, e-cash, and e-cheques!

The evolution of the internet and the World Wide Web has facilitated all manner of e-commerce. The emergence and dominance of the internet in the 21st century has also challenged the traditional legal mechanisms and the general legal infrastructure of doing business throughout the world.

2.5.1 Internet

As the name implies, the internet is a network of computers all over the world connected to each other either by telephone lines, fibre optic cables, or satellite network.[11] The *Australian Pocket Oxford Dictionary* defines internet as:

> "international computer network linking computers from educational institutions, government agencies, industry, etc., accessible to the general public via modem links."[12]

Wikipedia states that as of 31st March, 2008, 1.407 billion people use the internet. The internet is now accessed through mobile phones, data cards, and even through handheld game consoles from virtually anywhere in the world.[13] This of course now raises very challenging issues in terms of enforcement of legal rights and attaching liabilities – mainly jurisdictional issues.

2.5.2 World Wide Web

In general conversation, the internet and the World Wide Web are used somewhat interchangeably as if these two are the one and same. They are not the same. As seen above, the internet is the global communication system that provides the hardware and software infrastructure providing the required connectivity between computers whereas the World Wide Web is just one of the services transmitted via the internet.[14]

For the purposes of this Draft Report, we adopt the following definition from the *Australian Pocket Oxford Dictionary*:

---

[11] See Forder J and Q Patrick (2001) *Electric Commerce and the Law* (John Wiley & Sons Australia, Ltd) p.5.

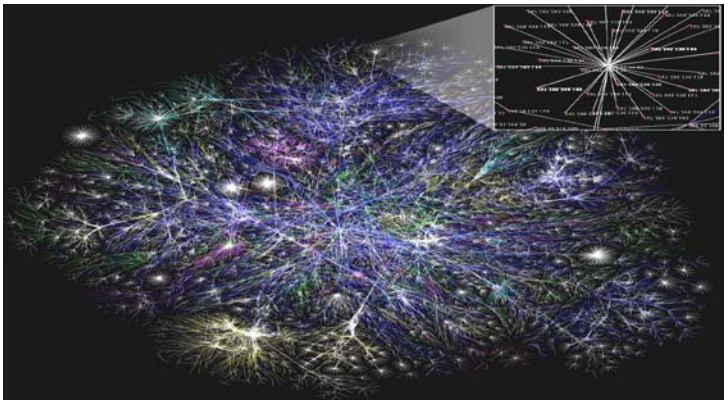
[12] The Australian Pocket Oxford Dictionary, fifth edition, Oxford University Press, 2004

[13] Ibid

[14] http://en.wikipedia.org/wiki/Internet accessed at 3 October 2008

> "The World Wide Web is defined as visually-based system for accessing information (text, graphics, sound and video) by means of the internet, which consists of a large number of 'documents' tagged with cross-referencing links by which the user can move between sources"[15]

The image below gives an indication of what a fraction of the World Wide Web looks like:



Source: Wikipedia (http://en.wikipedia.org/wiki/Internet).

2.5.3 Electronic Commerce

"Electronic Commerce" or e-commerce for short is now appealing, attractive, and trendy. For most small to medium enterprises, it presents a cheaper option of doing business. Significant overhead costs in office and additional labour requirements are eliminated with the use of this mode of doing business.For many, through this mode, business can be conducted from the comfort of ones home! What then is e-commerce? In very broad terms, e-commence may refer to and include "all commercial activity conducted with the aid of electronic devices. This definition may include:

- contracts concluded by telephone, telex or fax machine;

[15] The Australian Pocket Oxford Dictionary, fifth edition, Oxford University Press, 2004

- purchases made using electronic funds transfer at point of sale (EFTPOS), or even
- any transaction involving a card that uses electromagnetic data such as prepaid phone card.[16]

In a more narrower and somewhat technically acceptable form – and for the purpose of this Draft Report, the definition we adopt – is that e-commerce relates to the subset of all transactions conducted using computers connected to each other[17] by utilizing the internet and the World Wide Web. This definition we adopt recognizes and takes account of the impact of the internet and the World Wide Web in the manner in which people from very faraway places across the globe are now able to do business and transact across countries of the world with diverse legal systems. Various legal issues of concern emerged in the home countries. This is exactly the background against which this Reference was issued to us.

Electronic commerce has not really taken off here in PNG. In the region, particularly in Australia and New Zealand, the buying and selling of goods and services on the internet is very popular. Companies like *e-bay* in USA are selling virtually anything and everything on the internet. Michael Richardson predicted that:[18]

> "With internet use growing rapidly across Asia and the Pacific, the region is poised to become a big player in an electronic commerce market expected to be worth $US7 trillion by 2005."[19]

The same report, notes that:

> "In countries such as … Australia and Singapore, well over 40 percent of the population logs on regularly, while in poor APEC countries such as the Philippines and Papua New Guinea, less than 1 percent uses the web, mainly because of a shortage of equipment."

Indeed, this is one of the main reasons discouraging successful electronic commerce in PNG and the other Pacific Island countries.

---

[16] Forder J and P Quirk (2001) *Electronic Commerce and the Law* (Milton: John Wiley & Sons Australia Ltd) p.4

[17] Ibid at p.5

[18] *The Australian* on 24th November, 2005, at p.25

[19] Cited in Forder J and P Quirk (2001) *Electronic Commerce and the Law* (Milton Qld: John Wiley and Sons Australia Ltd) at p.13

E-commerce has yet to flourish in PNG. There is, however, encouraging signs that the volume of business conducted on the internet, mainly through e-mail communication has been strong and is growing. Hence, the need for law reform.

On October 19 2006, PNG conducted its first e-commerce web based transaction in PNG Kina on the website: http://www.esishop.com.pg.[20] The internet was, however, introduced into PNG in May 1977. There are four (4) internet service providers (ISP) in PNG today. They are all connected to the main internet gateway through Telikom PNG.[21]

2.6 Some Legal Issues Raised By E-Commerce

In thinking about the legal issues raised by e-commerce which we address in the later part of this Draft Report, it is important at the outset to differentiate, on the one hand, those possible issues which may arise within our jurisdiction (i.e. PNG) and on the other hand, those many and more complex issues which may arise as a result of engaging in e-commerce outside of the jurisdiction (i.e. internationally). The main thrust of this Reference is aimed at the first instance – the concern about the proof of business and electronic records within PNG. However, most of the issues do overlap. The following are some of the legal issues and concerns that may arise:

- whether email correspondence between parties in an e-commerce transaction are admissible evidence within the terms of Sections 65-67 of the *Evidence Act*;
- whether unsigned contracts and unsigned accompanying emails are admissible evidence within Division 5 of the *Evidence Act* ;
- whether the scanned signatures onto emails and contract documents are admissible evidence within the terms of Division 5 of the *Evidence Act* Chapter 48, and
- does Division 5 of the *Evidence Act* provide room to authenticate and inject integrity and security into the use of scanned signatures on electronic contracts, official communications and emails, etc?

---

[20] See Ramamurthy S (2007) "*E-Commerce Opens Up World of Opportunities*" *2007 Papua New Guinea Year Book* (Port Moresby: Cassowary Books and Pacific Star Ltd) pp 94-97

[21] Ibid

Electronic commerce conducted covering two or more jurisdictions may raise some of the following legal issues:

- at what point and in which jurisdiction are the business transactions (contracts, etc) concluded?;
- what are the terms of the contract, especially concerning payment (as to how, when, where, or in which currency should the payments be made)?;
- the manner of delivery of the goods and services or the performance of the services;
- the remedies available to the parties if one party fails to fulfill the terms of the contract or the goods or services rendered are defective or unsatisfactory respectively, and
- the ever critical issue of jurisdiction or applicability of which laws or whose laws?[22]

It is, of course, apparent that the inter-jurisdictional issues raised by the advent of the internet, World Wide Web, and electronic commerce venture well beyond the capacity of the current Division 5 of the *Evidence Act* . For this reason PNG looks to the UNCITRAL *Model Law on Electronic Commerce* and the *Model Law on Electronic Signatures With Guide to Enactment* 2001 and some comparable legislation within the region such as the Vanuatu for guidance.

It may even be as one commentator puts it:

> "The matter raised in the paper as legal issues are simply a question for competent drafting of a document. Questions of jurisdiction, terms and method of payment and delivery and remedies available in default should always be clearly and expressly stated if there is ever the possibility of doubt.
>
> The Common Law contains many answers to such questions but the laws of interpretation can introduce an element of uncertainty at times. In view of the widespread ignorance in the commercial community on the operation of the private international law, prudent lawyers who wish to avoid negligence actions should draft clear and explicit documents. Legislations should be

[22] Adapted from Forder J and Quirk P (2001) *Electronic Commerce and the Law* (Milton, Qld: John Wiley and Sons Ltd) p.p 32-33

unnecessary if the profession and the commercial community take more care in the formulation of documents required by commerce."[23]

[23] Mr Goodwin Poole

3. Current Law and Practice on the Conduct of Business & Electronic Records

Contents

3.1 Introduction

The current law and practice in this area of concern is governed by the *Evidence Act* 1975, Chapter 48. On the whole, the law of evidence in PNG is based on the Common Law of England which now applies in PNG as part of the Underlying Law.

Business and electronic records fall under the category of real evidence or documentary evidence and are generally subject to the general rule against hearsay evidence, which is:

> "Evidence by any witness of what another person stated (whether verbally, in writing or otherwise) on any prior occasion is inadmissible for the purpose of proving that any fact stated by that other person on that prior occasion is true."[24]

In other words, the rule against hearsay evidence prohibits the production of the evidence by another person outside the court, only if the purpose of proposing to rely on the evidence is to attest to the truth of the statement made or written, but not the fact that such a statement was made or written.

3.1.1 Real Evidence

Real evidence is in a tangible form such as photographs, tape-recordings, readings, and other information produced by a mechanical devise such as a

[24] Murphy P (1980) *A Practical Approach to Evidence* (London; Blackstone Press Ltd) p.165;

computer.[25] To overcome the rule against hearsay evidence, statute law has intervened in most, if not all, common law jurisdictions by now ensuring that computer generated statements or documents may now be admitted as evidence as an exception to the rule against hearsay evidence.[26]

3.1.2 Documentary Evidence

Documentary evidence is any evidence that is in the form of document or such other written form. Wikipedia explains that "although this term is most widely understood to mean writings on paper (such as an invoice, a contract or a will), the term actually include any media by which information can be preserved. Photographs, tape recordings, films, and printed emails are all forms of documentary evidence."[27] The distinction between "real evidence" and "documentary evidence" is not in the form of the material evidence, but rather the purpose for and use of which the evidentiary material is made. Documentary evidence is required and relied upon for purposes of proof of the content of the document. However, if the appearance or shape of the documentary evidence – for example, a blood stained printed email message, is required for proof of the DNA of the assailant (rather than the content of the email message) – then the blood stained printed email message takes the form of real evidence rather than documentary evidence. Generally at common law, documentary evidence are subject to authentication – either by a eyewitness attesting to the execution of the document or to the testimony of a *witness to testify to the identity* of the author.

At common law, "documentary evidence is also subject to the best evidence rule, which requires that the original document be produced unless there is a good reason not to do so".[28]

Also at common law, there is a distinction between "private documents" on the one hand, and "public or official documents." Murphy notes that "a party who wishes to rely on the contents of a private document as direct evidence, must adduce 'primary' (as opposed to 'secondary') evidence of the contents of that document" and goes on to point out that the requirement for 'primary evidence' is a reference to 'original document'.[29] This distinction between "private documents" and "public or official documents"

---

[25] See n.1 at p.186;
[26] Ibid
[27] http://en.wikipedia.org/wiki/Documentary - evidence viewed on 15/10/2008;
[28] Ibid;
[29] See no.1 at p.501;

is reflected in our current *Evidence Act* where the Act does provide for the proof of public and official documents in Part IV of the Act. Public or official documents, which can be produced without being subjected to the various common law requirements as stated above in accordance with the relevant provisions of the *Evidence Act,* include the following:

- copies of any legislation or related instruments issued by printed by the Government Printer;[30]
- all documents relating to judicial proceedings;[31]
- votes and proceedings in Parliament;[32]
- Government Gazette and such other official publications printed by the Government Printer;[33]
- Secondary evidence of registered deed or document;[34]
- probate and letters of administration;[35]
- certificates relating to births, deaths and marriages;[36]
- documents relating to certificate of incorporation of a corporate entity;[37]
- official statistics published by the National Statistician;[38]
- business records;[39]
- computerized information and related computer generated statements,[40] and
- various certified copies of public documents issued and signed by the Registrar-General, Registrar of Titles or the National Statistician;[41]

[30] See ss.38, 39 & 40 *Evidence Act;*
[31] See ss.44-47 *Evidence Act;*
[32] See s.48 *Evidence Act;*
[33] See ss.52-53 *Evidence Act;*
[34] See s.55 *Evidence Act;*
[35] See s.56 *Evidence Act;*
[36] See s.57 *Evidence Act;*
[37] See s.58 *Evidence Act;*
[38] See s.59 *Evidence Act;*
[39] See s.61 *Evidence Act;*
[40] See ss.64-67 *Evidence Act;*

Some overtly private documents have also been somewhat exempted from the evidence rule by the *Evidence Act* – thus negating the requirement for the production of the original of a private document. The Act imposes some requirements that must be met before such documents are admitted. These documents include:

- documents processed by an independent processor;[42]
- prints ore re-prints from the negative of a document;[43]
- photocopies made from approved photocopy machines;[44]
- entries bankers books, accounts, journals, etc,[45] and
- business records, including a photographic or a photostatic reproduction of a document used in the regular course of business,[46] and
- computerized information [47] or computer generated statements.[48]

3.2 Proof and Admissibility of Other Public or Official Documents

Because of the broad based view we took of the term "business records" at paragraph 2.2 above, officially sanctioned documents may also constitute business records in given circumstances, particularly where members of the public rely on the document to do business. Without having to be exhaustive, such official documents we have in mind (in this context) include officially sanctioned and released government policy documents printed by the Government Printer, statistics or records released by the National Statistician, Certificates of Incorporation for companies, business groups, Incorporated Land Groups, Associations, documents concerning shareholding or ownership of companies held by the Registrar of Companies, and Certificates of Title to land or leases,etc.

Allowance is made for the production and admissibility of reproductions of public documents as certified reproductions with an adequate certification

---

[41] See ss.70-72 *Evidence Act;*
[42] See s.74 *Evidence Act;*
[43] See ss.75-81 *Evidence Act;*
[44] See ss.86-88 *Evidence Act;*
[45] See ss.91-94 *Evidence Act.*
[46] See 5.61 *Evidence Act;*
[47] See s.65 *Evidence Act;*
[48] See s.66 *Evidence Act.*

to its truthfulness or verification by a person in authority certifying it to be a reproduction under Section 70 of the *Evidence Act.* Section 70 (2) goes onto state that if the reproduction of the document bears a certification signed by a person having authority or custody of the document, then that is sufficient and the reproduction would be admissible without further proof. A "reproduction" is defined under Section 68 of the *Evidence Act* to mean, either a machining-copy (photocopy) of the document or a print made from a negative of the document.

3.3 Proof and Admissibility of Business Records

We have taken a broad based view of the term "business record" to include not only records of those relating to the conduct of commerce related business, but also business relating to public administration. Section 61(2) of the *Evidence Act* is a key provision relating to the proof and admissibility of business records. This provision says that any writing or a photographic or a photostatic reproduction of a document "purporting to be a memorandum or record of an act, matter, or event is admissible as evidence in a court as proof of the facts stated in it if it appears to the court that:-

(a) the memorandum or record was made in the regular course of a business at or about the time of the doing or occurrence of the act, matter or event, and

(b) the source of information, and the method and time of the preparation of the memorandum or record, were such as to indicate its trustworthiness."

Section 61(4) then further states that when considering the admissibility of such business records, the court must have regard to all the relevant circumstances, including:

- the source from which the business record is produced, and
- the circumstances of its receipt and custody by the person producing it or by any person from whom it has been obtained for the purpose of producing it in evidence.

If it appears to the court that it would not be in the interest of justice to admit into evidence any business record, then the court would be entitled to refuse admission of such business record.[49] In the exercise of its discretion in deciding whether or not to admit business records into evidence, the court is empowered not only to receive formal testimonial evidence "but

[49] See s.61(3) *Evidence Act*

may inform itself in any way that it thinks fit and particularly by the affidavit, oath, affirmation, or certificate of a person who professes to have knowledge of any of the matters to which the writing relates or of the circumstances relating to its preparation"[50]

Issues 3.3.1
Does s.61 of the *Evidence Act* allow for the admissibility and proof of business records capable of allowing for the admission and proof of electronic records as business records?

Submissions and Consultations

During the recent CLRC national consultation it was found that most of those consulted gave negative answers to this issue. Mr Goodwin Poole, in his submission on this issue stated that:

> "The short answer to this is NO because the section proceeds on the basis of "writing" rather than on the basis of "document". Document is defined in the *Evidence Act* in a manner which concentrates on the medium of reproduction and states that it,
>
> > includes a book, plan, paper, parchment or other material on which there is any writing that is marked with letters or marks denoting words or any other signs capable of carrying a definite meaning to persons conversant with them, and includes a part of a document.
>
> The definition makes the document admissible as a business record if it is a contemporaneous record, which on the face of it, is a "trustworthy" recording of something, which took place in the regular course of business.
>
> The whole issue of admissibility of records should be examined on the basis of reliability of the content received. The weight to

[50] See s.61(5) *Evidence Act*

be given should be a matter for the Court on examination of the facts of each individual case."

CLRC Views

The CLRC is of the same view as that of the others in that the definition does not allow for the admission and proof of electronic records as business records. Hence it is of the view that the solution to this issue could well be an expanded definition of document as:

"Any records of information including:

(i) Anything on which there is writing; or

(ii) Anything on which there are marks, figures, symbols, or perforations conveying a meaning to persons qualified to interpret them; or

(iii) Anything from which should, electronic impulses, radio waves, images or writings that can be reproduced with or without the aid of anything else; or

(iv) Any map, plan, drawing, or photograph."

This expanded provision should meet the need of electronic documents, especially if coupled with a revision, which explicitly deals with proof of the contents of documents. Such a provision now occurs in section 48 of the *Commonwealth (Australia) Evidence Act*.

(1) A party may adduce evidence of the contents of a document in question by tendering the document in question or by any one or more of the following methods:

(a) Adducing evidence of an admission made by another party to the proceeding as to the contents of the document in question,

(b) Tendering a document that:

(i) is or purports to be a copy of the document in question; and

(ii) has been produced or purports to have been produced by a device that reproduces the contents of documents.

(c) If the document in question is an article or thing by which words are recorded in such a way as to be capable of being reproduced as sound, or in which words are recorded in a

code (including shorthand writing) – tendering a document that is or purports to be a transcript of the words;

(d) If the document in question is an article or thing on or in which information is stored in such a way that it cannot be used by the Court unless a device is used to retrieve, produce or collate it – tendering a document that was or purports to have been produced by use of the device;

(e) Tendering a document that:

(i) forms part of the records of or kept by a business (whether or not the business is still in existence), and

(ii) is or purports to be a copy of , or an extract from or a summary of the document in question, or is purports to be a copy of such an extract or summary.

(f) If the document in question is a public document tendering a document that is or purports to be a copy of the document in question and that is or purports to have been printed:

(i) by the Government Printer or by the government or official printer of a State or Territory, or

(ii) by authority of the government or administration of the Commonwealth, a State, a Territory or a foreign country, or

(iii) by authority of an Australian Parliament, a House of an Australian Parliament, a committee of such a House or a committee of an Australian Parliament.

(2) Subsection (1) applies to a document in question whether the document in question is available to the party or not.

(3) If the party adduces evidence of the contents of a document under paragraph (1)(a), the evidence may only be used:

(a) in respect of the party's case against the other party who made the admission concerned; or

(b) in respect of the other party's case against the party who adduced the evidence in that way.

(4) A party may adduce evidence of the contents of a document in question that is not available to the party, or the existence and contents of which are not in issue in the proceeding, by:

(a) tendering a document that is a copy of or an extract from or summary of, the document in question; or

(b) adducing from a witness evidence of the contents of the document in question.

Such a provision has been or is under consideration or has been adopted by other Common Law jurisdiction and it would in the view of the CLRC be suitable to Papua New Guinea than solution evolved in non-Common Law jurisdiction.

Proposal 1: The definition of document be expanded to cover electronic documents.

3.4 Admissibility and Proof of Computerised Information

Provisions for the admissibility and proof of computer generated information and statements are made under Division 5 of the *Evidence Act*. For purposes of this Division, "computer" is defined as a device for storing and processing information[51] and any reference to a computer also includes a situation where there are more than one computer used to process and store information.[52]

For purposes of Division 5 of the *Evidence Act*, Section 64(3) goes on to explain that:

- a reference to information being derived from other information is a reference to its being derived from it by calculation, comparison or any other process; and
- information shall be taken to be supplied to a computer if it is supplied in any appropriate form and whether it is applied directly or (with or without human intervention) by means of any appropriate equipment; and
- where, in the course of activities carried on by a person or body, information is supplied with a view to its being stored or processed for the purposes of the activities by a computer operated otherwise

[51] See s.64(1) *Evidence Act*
[52] See s.64(2) *Evidence Act*

than in the course of activities, the information, if duly supplied to the computer, shall be taken to be supplied to it in the course of the activities; and

- a document shall be taken to have been produced by a computer whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment.

Concerning the specific matter of admissibility of computerised information, Section 65(1) of the Act says that: "In any legal proceedings a statement contained in a document produced by a computer is admissible as evidence of any fact, stated in the document, of which direct oral evidence would be admissible, if it is shown to the satisfaction of the court that:

- the document containing the statement was produced by the computer in the course of a period during which the computer was used regularly to store or process information for the purposes of activities regularly carried on over that period, whether for profit or not; and
- during the period there was regularly supplied to the computer, in the ordinary course of those activities, information of the kind contained in the statement or of the kind from which the information so contained was derived; and
- throughout the material part of the period the computer was operating properly or, if not, that any defect in its operation during that part of the period was not such as to affect the production of the document or the accuracy of its contents; and
- the information contained in the statement reproduces or is derived from information supplied to the computer in the ordinary course of those activities.

One of the main issue for us to consider in this Reference is: are the information obtained from internet or e-commerce transaction generated information through websites capable of being accommodated under Section 65(1) of the *Evidence Act* as being computerised information since their source is the computer? It is obvious that when Section 65 of the *Evidence Act* was drafted in 1975, the current websites and e-commerce generated information and email were non-existent and therefore their inclusion within the current Section 65(1) *Evidence Act* was never envisaged. The question then is: is the current Section 65(1) *Evidence Act* broad enough to accommodate the admissibility and proof of email;

information and documents relating to e-commerce transactions through websites on the internet?

Submissions and Consultations

During the nation-wide consultation it was noted that although some of the stakeholders consulted gave a negative answer to this issue, others argued in the affirmative. The New Britain Palm Oil Legal Officer was one of those who argued in the affirmative stating that:

> "Section 65 of the *Evidence Act* is adequate to tackle the electronic world issue. The *Companies Act* has already harnessed the provision and has allowed for the proof of electronic records."

Mr Daniel Kaima in his submission on this issue stated that although Division 5 of Part IV of the Act appears wide enough to cover information and documents produced through electronic transactions using websites, new and modified definitions of common evidentiary terms should be incorporated in the Act to set the basis for the application of Division 5 to effectively cover admission and proof of information and documents relating to e-commerce transactions conducted through websites.

He submitted that the collective effort of sections 64 and 65 of the Act implies that a proponent who intends to tender a document produced by a computer must adduce evidence to the satisfaction of the court that the document was produced in the course of a period during which the computer was regularly used to store or process information, that during the period and in the ordinary course of activities the document was derived, and throughout the material part of the period the computer was working properly or that any defect did not affect the production or accuracy of the document, and the document was reproduced from the information supplied to the computer in the ordinary course of storing and processing information.

Under Section 65(2), courts are given a wide discretion to draw any reasonable inference from the circumstances in which the document is produced as well as other considerations, including the form and content of the document in question. Along with section 66 of the Act, Sections 64 and 65 not only provide a general ambit to capture electronic records generated and stored by a computer as defined in the Act, but rather than relying on the face value of a document in question obliges a proponent to adduce evidence in favour of the prerequisites for reliability in Section 65(1) and 65(2) and the authenticity requirements in Section 66(1) and 66(2) before the document can be admitted as evidence. As in any common

law jurisdiction, in a criminal matter, if the proponent is on the prosecution side, he or she has the burden of proving these reliability and authenticity requirements beyond a reasonable doubt. If, however, he or she is defending, the onus is set on the balance of probabilities. If the matter is civil, the onus and burden will be on the proponent to establish these requirements on the balance of probabilities.

Section 67 of the Act further empowers a court to have regard to all the circumstances from which an inference can reasonably be drawn as to the accuracy or otherwise of a material statement, and whether the information contained in the statement was derived from was supplied to the computer. It also questions whether any person concerned with the supply of information to the computer or the operation of the computer or of equipment by means of which the document containing the statement was produced by it had any intent to misconceive or conceal the fact to be proved.

Thus, a court is not only required to question the admissibility of computer generated records under Section 65 and 66 as a matter of procedure, but as a matter of substance. It is also mandated to question the accuracy and the source of the information contained in the material statement in a record, as well as the intent behind the supply of the information, the operation of the computer, or the equipment by which the record containing the information was produced.

It follows that if a proponent wishes to rely on a computer-generated record from the information processing system such as the network server of an internet service provider or the database system of a content host of the website the subject of proceedings, he or she would have to ensure the requirements of section 64, 65, 66, and 67 of the Act are met and accordingly employ foreign case laws to legally contend that these requirements are met in the specific circumstances he or she intends to admit the information or document as evidence.

CLRC Views

The CLRC is of the view that Section 65 of the *Evidence Act* is not adequate. It only allows for the admissibility of documents produced by a computer in the regular course of business or activities. It does not extend to situations where the computerized information is produced from website, which often are done not in the regular course of business, but as a one off thing by anybody who has excess to the internet at any given time.

Furthermore, while technology of information transmission alters because of the advances in the medium of communication, the problem which the law and the commercial community must address is not the medium of communication, but the authenticity of the content received. Just as written communication is accepted as generally more accurate than oral transmission of information because of the certainty of the content. So when checking the authenticity of information transmitted electronically, the prime concern should be the reliability and trustworthiness of the content that was received. If this is to be done then the issue cannot be wholly addressed by inserting new subsections into this provision. The issue could be well addressed if e-commerce transactions are addressed in a separate new legislation to be known as an *Electronic Transactions Act*. The consequential effect of this new legislation is that it will facilitate the growth of electronic commerce and at the same time address all electronic and digital transactions using any medium of information transmission.

Proposal 2: A new legislation should be enacted to be known as the Electronic Transaction Act, which should then house all electronic transactions conducted through any medium of information transmission. This new legislation will also effectively cover admission and proof of information and documents relating to e-commerce transactions conducted though websites and any other mediums of electronic communication.

3.5 Admissibility and Proof of Computer Generated Statements

Section 66 of the *Evidence Act* provides for the admissibility and proof of computer statements. As we saw earlier, under Section 64 (3)(d) of the *Evidence Act*, a document is deemed to have been produced by a computer irrespective of whether the document was produced by a computer with or without human intervention, but by the utilization of appropriate and normal equipment. In this regard "normal equipment" in our view is a reference to both hard ware and software associated with servers, networks, all computer parts and accessories, cables and printers, etc.

Section 66 of the *Evidence Act* is as follows:

"66. Proof of Computer Statements:

(1) Where in any legal proceedings a statement contained in a document is proposed to be given in evidence under this Division it may be proved by the production of the document or (whether or not the document is still in existence) by the production of a copy of the document, or of the material part of the document, authenticated in such manner as the court approves.

(2) Where in any legal proceedings it is desired to give a statement in evidence under this Division, a certificate –

- identifying the document containing the statement and describing the manner in which it was produced; or
- giving such particulars of any device involved in the production of the document as are appropriate for the purpose of showing that the document was produced by a computer; or
- dealing with any of the matters referred to in Section 64(3),

and purporting to be signed by a person occupying a responsible position in relation to the operation of the relevant device or the management of the relevant activities (whichever is appropriate), is evidence of any matter stated in the certificate.

(3) For the purposes of Subsection (2) it is sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it.

In essence, the thrust of Section 66 of the *Evidence Act* is concerned with the authentication of the document in the form of a computer statement, such as a print out from a computer via a printer and the issue of authentication is left to the court to settle through whatever method it may wish to adopt. One of the method identified to ensure authentification is through the issuance of a certificate to identify the document containing the statement and describing the manner in which it was produced and signed off by the responsible staff such as the computer manager or IT officer with supervisory oversight over the computer network or the server.

Section 67 of the *Evidence Act* provides for varying degree of weight to be given by the courts when admitting into evidence computer statements by taking into consideration the following circumstances:

- whether or not the accuracy of the statement is in any doubt;
- whether or not the information contained in the statement reproduces or is derived from was supplied to the computer or was recorded to be supplied to the computer contemporaneously with the occurrence or existence of the facts dealt with in the information, and
- whether or not any person concerned with the supply of information to the computer, or the operation of the computer, or of equipment by means of which the document containing the statement was produced by it – had any incentive to conceal or misinterpret the facts.

The issue for us to address in this Reference is whether electronic records and electronic communications such as email can be construed as "computer statements" and therefore falling within the ambit of the current Section 66 of the *Evidence Act*. If not, then how best should we provide for the admissibility and proof of electronic records and electronic communications?

Submission and Consultations

During the nationwide consultations, the majority of those consulted were of the view that Section 66 of the *Evidence Act* is not wide enough to allow for proof of electronic records and electronic communication. Mr Daniel Kaima submitted that section 66(1) obliges the courts to provide for the manner in which to authenticate the original, copy or a material part of the document in question as a requisite to producing the document as evidence in court, and Section 66(2) entails the use of a certificate to *inter alia* identify the document and the manner in which it was produced or provided particulars of any device involved in the production of the document.

Section 66 appears merely to empower the courts to, considering the circumstances, determine a checklist process for authenticating a document or a part of it for admission purposes. Although provision is made for establishing a specific process for admissibility of an electronic record or record of electronic communication, the question of what criteria courts would use to determine an applicable checklist process remains unanswered. Issues such as to what extent can courts consider the 'Best Evidence Rule,' and how should an 'original,' 'copy' or material part of an

electronic record or record of electronic communication satisfy current accepted standards of the form and manner in which accepted evidence are held, are some of the important procedural considerations that courts need to b e guided by in determining a specific process.

CLRC Views

The CLRC is of the view that Section 66 of the *Evidence Act* is not wide enough to allow for proof of electronic records and electronic communication. Electronic records as stated earlier could well be resolved for its admissibility by an expanded definition of the word "document". Electronic communication on the other hand involves a lot more issues and should be addressed by creating a new legislation to be called *Electronic Transaction Act*. This legislation will provide a regulatory framework that recognises the importance of the information economy to the future economic and social prosperity of PNG, facilitates the use of electronic transactions, promotes business and community confidence in the use of Electronic transactions, and finally enables business and the community to use electronic communications in their dealings with government.

4. Electronic Transactions and Electronic Records

Contents

4.1 Introduction

This part of the Report focuses on electronic communication. We will also focus our discussion on electronic documents that are often referred to as electronic records and how these could be accommodated within the *Evidence Act* or related legislation in PNG. Electronic and digital signatures, which present their own peculiar issues will also be considered, including the forms electronic signatures can take and why we should consider legislating the use of electronic signatures.

4.2 Electronic Communication

Electronic communication is defined in part two of the Report. The definition of 'electronic communication' is adopted from the Australian *Electronic Transactions Act* 1999, which is based on the UNCITRAL *Model Law on Electronic Commerce*. The term "electronic communications" therefore embraces the mediums and facilitators of communication that involve: emails, websites, chat rooms, and electronic data interchange mediums, social networking sites, and virtual worlds.

The email, the list serve, and chat-rooms are mediums that facilitate or provide for the transmission of electronic messages between computers, or in more recent times, even to mobile phones that transmit text, photo, and video messages and allow for transfer of such messages to standard computers, as well as personal digital assistants (PDAs) that can copy SMS messages into an email or word processing documents.[53]

In all these mediums, messages created by the user are converted into electrical signals, which are then generated as electromagnetic waves or as a sequence of voltage pulses that travel along a physical path that carries a signal between a signal transmitter and a receiver called the transmission medium, which can be guided (wirings, optical fibre cables) or unguided (earth's environment used as physical parts to carry electronic signals) mediums. The focus of the law of evidence here is the message itself and how that message can be produced as evidence. As we saw in Chapter 3 above, the existing *Evidence Act* provisions only deal with computerized information and computer generated statements, but clearly not electronic communications generated by medium other than a computer. There is therefore a gap in the law of evidence in this regard.

4.3 Electronic Records

States that have enacted laws that promote and advance e-commerce have always been faced with one major challenge that is, how to legislate electronic documents, often referred to as "records" or "electronic records" and "signatures" that are created, communicated and stored in electronic form. These signatures may either be electronic signatures or digital signatures.

The exchange of messages is entirely web based. Most web providers and web hosts are required, through appropriate computer programs, to maintain records of the interaction between the subscribers to these websites and the

---

[53] See for instance, the *Council of Europe Convention on Cyber Crime* 2002, which, rather than defining a 'computer', defines a 'computer system' as a device consisting of hardware and software developed for automatic processing of digital data. And 'computer data' is confined to data kept in such a form that it can be directly processed by the computer system, i.e., the data must be electronic or in some other directly processable form; see Council of Europe, 'Council of Europe Convention on Cyber crime', opened for signature on 23 November 2001, Europe. T.S. No. 185 (2002); <http://conventions.coe.int/Treaty/EN/Projects/FinalCybercrime.htm> at 17 February 2009. For a discussion of the requirements of the convention pertaining to the preservation of electronic evidence, see Mike Keyser, 'The Council of Europe Convention on Cyber crime' (2003) 12 *Florida State University Journal of Translational Law and Policy* 287.

interaction between these websites and a particular subscriber.[54] These electronic records created, communicated, and stored in electronic form and electronic records from computer programs such as the Microsoft Office program as well as records created by computers without human input can be made to be subject to either a specific law or the law of evidence in general.

The question is how best can this done, given the fact that the current *Evidence Act* and related status lack the coverage of this subject. The advancement of e-commerce in PNG may require the enactment of an appropriate legislation that should take a technology neutral approach and at the same time save individuals, companies, corporations, and the Government from unnecessary costs, embarrassment, and pitfalls.

Accordingly, legal recognition to electronic records is the main focus here – and perhaps could also extend to cover the other electronic documents like electronic and digital signatures.

4.3.1 Need for legal recognition of Electronic Records as Evidence

It is necessary to ensure that provisions are made for the legal recognition of electronic records and to facilitate the admission of such records into evidence in legal proceedings. The current scope of the *Evidence Act* does not adequately provide for the use of the term electronic records and electronic communication. Tape recording of evidence, although in many places is not admissible as evidence are categorized as electronic record. New generation mobile phones that have an email/internet capacity can also be used to create electronic record, as well as through text messaging. There are many voice recording devices as well as telephone voice mail that can produce electronic record. It is presumed that electronic record can be written or printed out as video tapes, CD ROMS, DVD, and hard copy. Sound recordings can also be "edited" and reproduced, as can composite devised images on the computer. Scanned and photocopied documents can become electronic records. New telephone equipment that has an internet facility does likewise. Video cameras and electronic surveillance cameras/equipment produce digital evidence.

---

[54] See for instance, s 11 of the New South Wales *Electronic Transactions Act* 2000, s 12 of Australia's *Electronic Transactions Act* 1999 (Cth), Article 10(3) of the European Union's *Electronic Commerce Directive* 2000, s 146 of the *Uniform Electronic Transactions Act* 1999 (United States) and s 147 of the *Electronic Signatures in Global and National Commerce Act* 1999 (United States).

Most of the people we interviewed stressed that our legislation has not kept up with modern technology and software systems. However, current law practice incorporates modern process and therefore there is a need for specific treatment of electronic records.

Most people we interviewed in our Port Moresby based survey stated that the process of interpretation, statutory writing requirement, delivery requirement, original document requirement, retention requirement, and admissibility/proof and weighting need to be adjusted to reflect technological changes. The processes attached to accuracy, authenticity, and weight of evidence is paramount as they are and should be fully locked into admissibility of evidence.

Also there is a need to define what devices – computers, videos, DVDs, CDs, mobile phones etc, that are considered acceptable for presenting (by laws) evidence that is considered legally reliable. Most businesses have access to such equipment and could provide records electronically. There may be the need to authenticate a scanned original document on occasion to avoid concealment or misrepresentation of facts. Changes to acceptance of a wider range of electronic record would avoid massive print files in court presentations.

In relation to photographic, machine reproductions, or electronic images changes to the law must reflect current technologies such as colour photocopies, scanners, video cameras, digital cameras, and other equipment capable of high resolution images and copies.

The issue of data security and penalties for falsification, illegal copying, or alteration of original electronic documentation needs to be addressed. In considering these issues we should look at comparable legislation such as the Vanuatu *Electronic Transaction Act*[55] (2000) to see how they have legally addressed and accommodated electronic records under their legislation. The Vanuatu legislation is based on the UNCITRAL Model Law on Electronic Commerce.

[55] Steven E. Blythe, "South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga" 2006<http://www.paclii.org/journals/fJSPL/vol10/2.shtml#fn71> at 18 April 2009

4.3.2 The requirements for Electronic Transactions and records under the UNCITRAL Model Law

Under the UNCITRAL Model Law on Electronic Commerce the following are key considerations or requirements for electronic records:

a) Mere fact of electronic form must not deny recognition

Legal recognition, accuracy, 'admissibility or enforceability' must not be denied by law simply because:

- the information is in electronic form; or
- is referenced in an electronic record which purportedly results in such legal effect.[56]

b) Electronic records deemed to comply with requirement to be 'in writing'

Where a law or statute requires information to be in writing in order to be recognized, or characterizes information as mandated to be in written form, the electronic form will suffice if:

- it is "accessible;" and
- it can be retained for use at a later time.[57]

c) Electronic records deemed to comply with delivery requirement

Where a law states that information must be delivered to a person, that requirement will be deemed met if the information is in the form of an electronic record, and:

- the sender of the electronic record requires the receiver to acknowledge it; and
- the receiver acknowledges the receipt of the electronic record. This will hold regardless whether the law creates an affirmative obligation for delivery or the law warns of resulting effects if the delivery is not made.[58]

d) Electronic records to comply with signature requirement

Where a law states the affixation of a person's signature on a paper document, this will be met by an electronic record provided:

---

[56] Ibid
[57] Ibid
[58] Blythe, above n

- some means is employed to identify the person and to show that 'intended to sign or otherwise adopt' the electronic record's information; and
- the means used is reliable, in consideration of the reason for creation of the electronic record or the communication of it, or any 'relevant agreement.' This will be the case regardless of whether there is an affirmative duty to sign, or the law provides deleterious results if a person fails to sign.[59]

Electronic signatures supported by a certificate issued by an accredited Certifying Authority (CA) will definitely comply with a law's requirement for a signature on a paper document. However, an electronic record meeting these requirements will not be refused 'legal effect, validity, and enforceability' merely because:

- it is not an E-signature; or
- it is not supported by a Certificate.[60]

e) Electronic records deemed to comply with original requirement

Where a law states that an original paper document must be presented in order to meet a legal requirement, or if the law requires that a paper document must be stored in its original form, that requirement is met if:

- there is a 'reliable assurance' that the electronic document, from the time of its creation until the present, has not been altered; and
- if required to be presented, the information contained in the electronic record will be an accurate representation of the original. This rule holds regardless of whether there is an affirmative duty for presentation or retention in the original form, or the law dictates consequences if the original is not retained or presented.[61]

f) Electronic records deemed to comply with retention requirement

If electronic records are required by law to be stored, that requirement will be complied with by the storage of records in electronic form, provided:

- the information is accessible and can be stored for reference at a later date;

---

[59] Ibid
[60] Ibid
[61] Ibid

- the format used in the electronic form is identical to the one in which it was 'generated, sent or received,' or the format is a correct depiction of that information; and
- the location and date of the transmission and reception is also stored.[62]

g) Admissibility of Electronic Records and Evidential Weight Granted

The rules of evidence must not be interpreted in such a manner that the courts would refuse to admit an electronic record into evidence:

- merely because of its electronic form, or
- merely because it is not in its original form.

Factors to consider in the determination of the evidential weight when deciding on the admission of an electronic record include:

- the degree of trust and reliance that can be given to the electronic record, taking into account the means of generation, storage, and communication;
- whether the electronic record's integrity has been maintained since it was created, i.e., the trustworthiness of the record and whether there is assurance that it has not been altered;
- the means of identification of the sender, and
- other relevant factors.

4.4 Electronic Signature

This part of the paper begins with an overview on the nature and form of electronic signatures, its history, and issues relating to electronic signature evidence generally.

It is our view that legislating the use of electronic signatures is likely to serve as a vehicle for advancing e- commerce. If we fail to give legal recognition to electronic signatures in our jurisdiction, then such a failure may lead to unnecessary costs in the event of a dispute. Electronic signatures are increasingly being used and as such their validity is bound to be an issue for consideration in the near future.

[62] Ibid 6

Every person that uses an email account, electronic banking card, (kundu or save card), debit card or credit card, and do online transactions uses a form of electronic signature.[63]

Many countries throughout the world have enacted legislation to facilitate commerce by the use of electronic records or signatures in interstate and international commerce. Normally the intent is to ensure the validity and legal effect of contracts and other transactions entered into online or electronically.[64] A signature, whether electronic or on paper is first and foremost a symbol that signifies intent. The main focus is of course on the intention to authenticate which distinguishes a signature from an autograph.[65]

We point out that currently our laws do not provide for electronic signatures. The question then is should we enact a law to regulate electronic signatures?

4.4.1 Brief Historical Background

Before the American Civil War began in 1861, Morse Code was used to send messages electronically by telegraphy. Some of these messages were agreements to terms that were intended as enforceable contracts. An early acceptance of the enforceability of telegraphic messages as electronic signatures came from the New Hampshire Supreme Court in 1869.[66]

In the 1980s, many companies and even some individu als began using fax machines for high-priority or time-sensitive delivery of documents. Although the original signature on the original document was on paper, the image of the signature and its transmission was electronic.

Courts in various jurisdictions have decided that enforceable electronic signatures can include agreements made by email, entering a personal identification number (PIN) into a bank ATM, signing a credit or debit slip with a digital pen pad device (an application of graphics tablet technology) at a point of sale, installing software with a click wrap software license

---

[63] Steven Mason, "Electronic Signatures in Law" (Tottel, 2nd Edition, 2007) <http://www.stephenmason.eu/books/electronic-signatures-in-law/ > at 18 December 2008

[64] From Wikipedia, the free encyclopedia "Electronic Signature"<http://en.wikipedia.org/wiki/Electronic_signatures> at 18 December 2008

[65] Ibid

[66] Ibid

agreement on the package, and signing electronic documents online.[67] These electronic signatures therefore can take the various forms as discussed below.

4.4.2 What Constitutes an Electronic Signature

The main concern for electronic signature legislation is the authenticity of electronic documents, often referred to as "records" or "electronic records" and "signatures" which are created, communicated and stored in electronic form. These signatures are referred to as either electronic signatures or digital signatures.

The term 'electronic signature' is a generic, technology-neutral term that refers to the universal methods by which one can "sign" an electronic record. Although all electronic signatures are represented digitally (i.e., as a series of ones and zeros), they can take many forms and can be created by many different technologies. Examples of electronic signatures include: a name typed at the end of an e-mail message by the sender; a digitized image of a handwritten signature that is attached to an electronic document (sometimes created via a biometrics-based technology called signature dynamics), a secret code or PIN (such as that used with ATM cards and credit cards) to identify the sender to the recipient, a code or handle that the sender of a message uses to identify himself; a unique biometrics-based identifier, such as a fingerprint or a retinal scan, and a digital signature (created through the use of public key cryptography). [68]

4.4.3 Forms Electronic Signatures Can Take

The use of electronic signatures pre-dates any form of legislation. Towards the end of the twentieth century adjudicators found themselves applying well established legal principles to new technologies when presented in the form of electronic signatures, just as judges in the nineteenth century were confronted with the increasing use of printing, typewriting, and telegrams. There were no special legislation to accommodate those changes. Nevertheless, as highlighted below, there are different forms of electronic signature and the area of law where the particular form of signature has been held as an enforceable form of signature to prove the validity and legal effect of the nature of transaction entered into electronically.[69]

---

[67] Ibid

[68] Thomas J. Smedinghoff and Ruth Hill Bro, "Electronic Signature Legislation" 1999 <http://libraryfindlaw.com/1999/Jan/1/241481.html> at 14 April 2009

[69] Steven Mason, "Electronic Signatures in Law" (Tottel, 2nd Edition, 2007) <http://www.stephenmason.eu/books/electronic-signatures-in-law/ > at 18 December 2008

1. Typing a name into an electronic document

When a person types his or her name onto a file in electronic format, such as an e-mail, the text added can amount to a form of electronic signature. Clicking the 'I accept' or 'I agree' icon when buying goods or services on-line, or when installing software on a computer for the first time, the buyer is invariably required to click on the 'I accept' icon. This action has the effect of satisfying the function of a signature. Even if the act of clicking on an icon to order goods or services is deemed to be less secure than that provided by a manuscript signature, it does not follow that the reliability of the signature will affect its validity.[70]

2. The 'click wrap' method of indicating intent

Click wrap signatures do not require any form of legislation, yet this particular form of signature remains a form of electronic signature, despite the imposition of a highly technical response by way of legislation to what is a relatively simple legal issue. For lawyers, the central issue will be how to prove the nexus between the applications of the signature, (whatever forms it takes) and the person whose signature it purports to be.[71]

Clicking the 'I accept' or 'I agree' icon to confirm the intention to enter a contract when buying goods or services electronically has for a long time been a very popular method of demonstrating intent. In itself, the action of clicking the icon has the effect of satisfying the function of a signature. There have not been many cases relating to this very early form of electronic signature.

3. Personal Identification Number (PIN)

The PIN has become a very widely used form of authentication, especially to obtain access to a bank account through the use of an ATM (automated teller machine or automatic teller machine or automated banking machine or cash machine), or to confirm a transaction with a credit card or debit card. Invariably, a claim by the user that one or more transactions conducted on the account were not authorized by them will require the relying party to prove the transaction was authorized by the account holder. The fact a withdrawal or other form of transaction took place may not be in issue, and in any event, the bank can adduce the evidence under the relevant

---

[70] S.W.Mason, "Approaches to Electronic Signature" <**http://www.pravo.by/leginform/pdf/0105/mason.pdf**. >**at 29th May 2009**

[71] Ibid

business records or the Bankers' Books exemptions.[72] The issue is essentially one of consent and authorization by the account holder.

In this regard, we cite a District Court matter in *Roni v. Kagure* (DC No. 84 of 2004) where his Worship, Seneka found and held that the Defendants were negligent in failing to effect a stop to transactions to the complainant's account from being fraudulently made by a person who found the complainant's EFTPOS card over one weekend. His Worship further held that they failed to act on specific and unequivocal instructions from the complainant to effect stop payments and as a result of their negligence or even deliberate inaction, the complainant lost K5, 911.50 from withdrawals. Accordingly the defendants were held liable.

4. The name in an e-mail address[73]

The name in an e-mail address is capable of identifying a person, especially where an e-mail address is in an organization. This is because an email address is allocated by setting out the name of the person followed by the domain name of the organization. There are other variations that can be used, such as when an e-mail address describes the office or function of the person, rather than their name. However, even this, if allocated to a single person, can be used to identify a particular person. The link between the prefix of the e-mail address and the person responsible for sending the e-mail can be problematic. For instance, the sender may be able to choose the first part, and may decide to adopt letters or numbers or a combination of letters and numbers with a view to obfuscating their identity and the true e-mail address might be hidden by the sender. If it is not obvious who the sender was, and if correspondence ensues and a dispute occurs, it will be a matter of establishing what, if any, evidence there is pertaining to the source of the relevant e-mails as a preliminary point. It has been held in a number of jurisdictions that the name in an e-mail address or the combination of the name and the domain name in an e-mail address can be a form of electronic signature.

5. Scanned manuscript signature[74]

A variation of the biodynamic version of a manuscript signature is where a manuscript signature is scanned from the paper carrier and transformed into digital format. The files containing the representation of the signature can

---

[72] Ibid
[73] Steven Mason, "Electronic Signatures in Law" (Tottel, 2nd Edition, 2007) <http://www.stephenmason.eu/books/electronic-signatures-in-law/ > at 18 December 2008
[74] Ibid

then be attached to a document. This version of a signature is used widely in commerce, especially when marketing, materials are sent through the postal system and addressed to hundreds of thousands, if not millions, of addresses. The aim here is to link a person to a document, and the person creating or adopting the document in electronic format must have the requisite intent, and their intent must be associated to the document in some way.[75]

6. Biodynamic version of a manuscript signature[76]

This method involves obtaining a digital version of a manuscript signature where a person writes his or her manuscript signature by using a special pen and pad. The signature is reproduced on the computer screen and a series of measurements record the behaviour of the person as they perform the action. The measurements include the speed, rhythm, pattern, habit, stroke sequence and dynamics that are unique to the individual at the time they write their signature. The subsequent electronic file can then be attached to any document in electronic format to provide a measurement of a signature represented in graphic form on the screen.

7. Digital signature

A digital signature is a term for one technology – specific type of electronic signature. It involves the use of public key cryptography to sign a message, and perhaps is the one type of electronic signature that has generated the most business and technical effort, as well as legislative responses.[77] A "digital signature" is an electronic identifier that utilizes an information security measure, most commonly cryptography, to ensure the integrity, authenticity, and non-repudiation of the information to which it corresponds. Cryptography refers to a field of applied mathematics in which digital information may be transformed into unintelligible code and subsequently translated back into its original form. In public key cryptography or asymmetric cryptography, an algorithmic function is used to create two mathematically related or complementary "keys." One key is used to code the information while the other is used to decode it. Cryptography can be used to ensure the confidentiality of data (i.e., encryption) and to verify the authenticity and integrity of transmitted data.

---

[75] S.W.Mason, "Approaches to Electronic Signature" <**http://www.pravo.by/leginform/pdf/0105/mason.pdf**. **>at 29th May 2009**

[76] Ibid

[77] Thomas J. Smeddinghoff and Ruth Hill Bro of Baker & Mckenzie LLP, Electronic Signature Legislation, http://library.findlaw.com/1999/Jan/1/241481.html >at 28th May 2009.

The advantage of public key cryptography is that it allows the confidential transmission of information in open networks where parties do not know one another in advance or share secret key information.[78]

A very simple explanation which may serve to illustrate how a digital signature works is that a digital signature can comprise two, key pair (a private key and a public key) and a certificate, which is usually issued by a third party such as a certification authority. When an electronic message is signed with a digital signature, the private key is used to associate a value with the message using an algorithm. The computer undertakes this task. The value, the message and a certificate, linking the key to the named person or entity, is then sent to the recipient. The recipient uses the public key to check that the value is correct by 'unlocking' the value created by the algorithm. A computer undertakes the entire operation. The only action required of the human being (in theory) is to cause the computer to associate the digital signature to the message.[79]

4.4.4 Evidential Issues Relating to Electronic Signature.

It can be stated that the form of an electronic signature will have a bearing on its legal and evidential effect. However, it should also be noted that the elements that make up the definition of an electronic signature, and the presumptions that apply, will also affect its legal acceptance in a given jurisdiction. The elements that make up the definition of an electronic signature can demonstrate difficulties for the international acceptance of a particular form of signature.[80] To ease these difficulties the following have been designed to ensure the requirements for trustworthiness and security concerns. It may apply both to electronic and digital signatures hence it is generally considered that, an electronic signature is legally effective as a signature only if it is:

- unique to the person using it;
- capable of verification;
- under the sole control of the person using it, and

---

[78] Albert Gidari, John P. Morgan and Perkins Coie, "Survey of Electronic and Digital Signature Legislative Initiatives in the United States, September 12, 1997, <http://www.ilpf.org/groups/digrep.pdf >at 28th May 2009

[79] S.W.Mason, "Approaches to Electronic Signature" **<http://www.pravo.by/leginform/pdf/0105/mason.pdf. >at 29th May 2009.**

[80] Ibid

- linked to the data in such a manner that if the data is changed, the signature is invalidated.[81]

The UNCITRAL Model Law on Electronic Signatures imposes the following requirements:

- an electronic signature must include a method to identify the signer;
- an electronic signature must include a method to indicate the signer's approval of the information contained in the message; and
- the method used must be as reliable as was appropriate for the purpose for which the message was generated or communicated.

For purposes of ensuring reliability and integrity in the utilization of electronic records or electronic signatures in e-commerce transactions, it is important that we set out in law the specific requirements to give legal validity to electronic documents and electronic signatures or as acceptable substitutes for paper based documents and ink signatures. It is also important that we specify statutory writing requirements, delivery requirements, original document requirements, and retention requirements.[82]

4.5 UNCITRAL Model Law on Electronic Commerce

The UNCITRAL Model Law on Electronic Commerce was developed to assist and guide governments to achieve uniformity in the promulgation of national legislation in this area. It offers nation states a set of internationally acceptable rules as to how a number of legal obstacles may be removed and how a more secure legal environment may be created for electronic commerce.

4.5.1 Objectives of the Model Law on Electronic Commerce

The use of modern means of communication such as electronic mail and electronic data interchange (EDI) for the conduct of international trade (transactions) has been increasing rapidly and is expected to develop further as the use of the internet becomes more widely accessible. However, the communication of legally significant information in the form of paperless messages may be hindered by legal obstacles to the use of such messages,

[81] Ibid

[82] Steven E. Blythe, "South Pacific Computer Law: Promoting E-Commerce in Vanuatu and Fighting Cyber-Crime in Tonga" 2006 Volume 10 2006 – Issue 1 *Journal of South Pacific Law* 19

or by uncertainty as to their legal effect or validity.[83] As such the key objective of the Model Law on Electronic Commerce is to overcome these legal obstacles that are the results from the increased use of electronic commerce by enabling and facilitating the use of electronic commerce.

Amongst other things, the Model Law on Electronic Commerce was adopted to remove uncertainty as to the legal nature and validity of information presented in a form other than traditional paper document by providing equal treatment to users of paper based documentation and to users of computer based information.[84]

The practical objectives of the Model Law on Electronic Commerce are summarized as follows:

- To enable or facilitate the use of electronic commerce;
- To provide equal treatment to users of paper based documentation and to users of computer based information;
- To help remedy disadvantages that stem from inadequate legislation at the national level, which creates obstacles to international trade, and
- To act as a tool for interpreting existing international conventions and other international instruments that create legal obstacles to the use of electronic commerce.

4.5.2 The Scope and Structure of Model Law on Electronic Commerce

The Model Law on Electronic Commerce does not give a specific meaning to the word 'electronic commerce,' but instead attributes a broad reference related to the means of communication. Thus, among the means of communication encompassed in the notion of electronic commerce are the following modes of transmission based on the use of electronic techniques:

- communication by means of EDI defined narrowly as the computer to computer;
- transmission of data in a standardized format;

---

[83] UNCITRAL Model law on Electronic Commerce with Guide to Enactment 1996 with additional article 5 bis as adopted in 1998, United Nations, < http://www.uncitral.org/pdf/english/texts/electcom/05-89450_Ebook.pdf> at 20 April 2009

[84] Ibid

- transmission of electronic messages involving the use of either publicly available standards of proprietary standards, and
- transmission of free-formatted text by electronic means for example through the internet.

The Model Law on Electronic Commerce was drafted to cater for modern communication techniques. The principles, however, on which the Model Law is based, as well as its provisions, apply also to less advanced communication techniques like telecopy and telex.[85]

A characteristic of electronic commerce is that it covers programmable messages, the computer programming of which is the essential difference between such messages and traditional paper based documents. As a matter of principle, no communication technique is excluded from the scope of the Model Law on Electronic Commerce, including future technical developments. Thus, the objectives of the Model Law on Electronic Commerce are best served by the widest possible application of its scope.[86]

The Model Law on Electronic Commerce is divided into two parts: one, dealing with general electronic commerce and the other one dealing with specific areas of electronic commerce.

4.5.3 Specific Parts of Model Law Relevant for Our Purposes

Part 1 of the Model Law covers three chapters. Chapter one of the Model Law on Electronic Commerce deals with general provisions, including sphere of application, definitions, interpretation, and variation by agreement.

The sphere of application of the Model Law on Electronic Commerce covers all factual situations where information is generated, stored, or communicated, irrespective of the medium in which such information may be affixed.

Chapter two deals with application of legal requirements to data messages covering legal recognition of data messages, incorporation by reference, writing, signature, originality, admissibility, and evidential weight of data messages, and retention of data messages.

Neighbouring countries such as Vanuatu and Australia have incorporated this part into their respective legislation. This part is relevant for our purpose of the Model Law.

---

[85] Ibid
[86] Ibid 18

Legal recognition of data messages embodies the principle that there should be no disparity of treatment between data messages and paper documents. Incorporation by reference is intended to provide guidance on how a legislation should aim at facilitating the use of electronic commerce, considering situations where certain terms and conditions, although not stated in full, but merely referred to in a data message, may be recognized as having the same degree of legal effectiveness as if they had been fully stated in the data message. *Writing* is intended to define the basic standard to be met by a data message in order to be considered as meeting a requirement that information may be retained or presented in writing or that information be contained in a document.

The main functions of a *signature* are:

- identify a person;
- provide certainty as to the personal involvement of that person in the act of signing, and
- associate that person with the content of a document.

In addition to the above, a signature can also be utilized for the following purposes, depending on the nature of the document that was signed:

- the intent of a party to be bound by the content of a signed contract;
- the intent of a person to endorse authorship of a text;
- the intent of a person to associate herself with the content of a document written by someone else, and
- the fact of the time when a person had been at a given place.

Originality is a nearly universal requirement for documents of title and negotiable instruments, in which the notion of uniqueness of an original is particularly relevant. There are also others like trade documents such as:

- weight certificates;
- agricultural certificates;
- quality or quantity certificates;
- inspection reports, and
- insurance certificates

These documents are not negotiable instruments or used to transfer rights or title. It may, however, be essential that they be transmitted in their original

form, so that other parties in international commerce may have confidence in their contents. Originality is regarded as stating the minimum acceptable form requirement to be met by a data message for it to be regarded as the functional equivalent of an original.

Admissibility and evidential weight of data messages generally provides for both the admissibility of data messages as evidence in legal proceedings and their evidential value. It establishes that data messages should not be denied admissibility as evidence in legal proceedings solely on the ground that they are in electronic form. In relation to the evidential weight of a data message, provision is made as to how the evidential value of data messages should be assessed.

Finally, retention of data messages establishes a set of alternative rules for existing requirements regarding the storage of information. It is intended to set out the conditions under which the obligations to store data messages might exist in a law.

Chapter three of the Model Law deals with communication of data messages, including formation and validity of contracts, recognition by parties of data messages, attribution of data messages, acknowledgment of receipt, time, place of dispatch, and receipt of data messages.

Part 2 of the Model Law contains a more specific set of rules dealing with specific uses of electronic commerce. It covers the carriage of goods, including actions related to contracts of carriage of goods and transport documents.

The *carriage of goods* was the context in which electronic communications were most likely to be used. This provision applies equally to non-negotiable transport documents and to transfer of rights in goods by way of transferable bills of lading. It does not apply only to maritime transport, but also to transport of goods by other means.

Actions related to contracts of carriage of goods establish the scope that would encompass a wide variety of documents used in the context of the carriage of goods. It covers all transport documents, whether negotiable or non-negotiable, without excluding any specific document.

Transport documents establish not only written information about the actions referred to above, but also for the performance of such actions through the use of paper documents. They are specifically needed for the transfer of rights and obligations by transfer of written documents. The provision is intended to ensure that a right can be conveyed to one person

only, and that it would not be possible for more than one person at any point in time to lay claim to it.

Consultations and Submissions

The majority of the stakeholders we consulted did not agree with adopting the model law stating that the model law should only be used as a guide for us in creating our own home grown legislation that will reflect circumstances prevailing in the country. Mr Goodwin Poole in particular made the following submissions:

> "The short answer to this is no. This section of the paper raises a number of issues such as the need for the legal recognition of electronic records as evidence, the need to change the law to reflect current technology such as colour photocopies, etc, the need to work on the presupposition that the mere fact of electronic form must not deny recognition, and a number of other issues which seem to concentrate more on the medium of transmission to the extent that the authenticity of the content is of secondary consideration."
>
> He stated further that a District Court decision relating to a personal identification number is called in aid of an argument on the use of personal identification numbers to authenticate a transaction instead of a decision on negligence. It is a repetition, but nonetheless important, to note that forgery by electronic scanning is very difficult to detect and this should be an argument to be considered of paramount importance when looking at the use of an electronic signature to identify a document. For reasons already stated the appropriate amendment to the present *Evidence Act* (and, in particular, expansion of things such as proof of the contents of documents (Section 48 of the *Commonwealth Evidence Act*) and proof of complex or voluminous documents (Section 50 of the *Commonwealth Evidence Act*) would more than answer the question adequately without burdening the profession and the public at large with yet another piece of legislation.
>
> The question of hearsay documents is made further complicated by electronic technology. This also has been addressed in the *Commonwealth Evidence Act* (Section 69) which may be summarised as stating that:

(i) An exception is made to the hearsay rule by evidence of a previous representation made which is certified (e.g. as a true copy) in such a way as to meet the requirement to the hearsay rule/

(ii) A hearsay document of course is admissible as evidence of the fact of its existence rather than as proof of its contents and of course should contain the exceptions previously referred to under Section 69 of the *Commonwealth Evidence Act*.

CLRC Views

The CLRC is of the view that a new Act should be adopted based on the Model Law on Electronic Commerce that will incorporate provisions pertaining to originality of evidence, reliability, and authenticity requirements as to whether transactions done in electronic form should not be denied legal effect solely because they are done in electronic form or using electronic means, timing and venue rules, default rules on conflict of laws principles and obligations on maintaining records of electronic transactions and communication. These are, but some of the concerns which underpin the effective application of the law on evidence to records of electronic transactions. As such by enacting a separate legislation based on the Model Law on Electronic Commerce to address these concerns is necessary to initiate an effective exclusionary process for considering the impartiality and probative value of electronic records and records of electronic communication as admissible evidence. Once these procedural requirements and concerns are addressed, the substantial requirements under Section 61 and Division 5 of Part IV of the Act and other laws on evidence can develop consistently with the procedural requirements to harmonize and maintain uniformity in affording appropriate legal recognition to electronic records and records of electronic communication overtime.

5. Issues

Contents

5.1 Introduction

In this Reference, the CLRC has been directed to review the current *Evidence Act* and determine how best this Act can be amended to provide for the admission and proof of business records and electronic records. The CLRC has also been directed to identify any gaps in our laws on evidence generally and propose appropriate legislative reform to address such gaps. We have reviewed the current law on evidence relating to the admissibility and proof of "business records" and "electronic records" under the current *Evidence Act* in Chapter 3 of this paper. From this review, it is our view that:

- Division 5 of the *Evidence Act* in its current form is inadequate to effectively provide for the admission and proof of "electronic records" in particular;
- there is no definition of the term "business record", but a definition of the word "business" only and for purposes of the application of Section 62 of the *Evidence Act* (provision dealing with "Business Records") it is unclear and unsatisfactory to stretch the term to include all types and forms of electronic records to fall within the ambit of Section 62 and be admitted as "business records";
- Section 65 of the *Evidence Act* that provides for the admissibility and proof of *a statement contained in a document produced by a computer* (i.e. computerised information) cannot be extended to include the admissibility and proof of all types of electronic transactions generated through electronic communication particularly so that when such electronic transaction and communication is not generated by a computer but through other mediums such as new generation smart mobile phones, flash drives, CDs, DVDs, internet, emails, or digital cameras. The point of contention here is – if the statement is contained in a document that was initially drafted on a medium other than a computer, but was eventually converted by a computer through an appropriate

software application and was then printed from a computer – does that statement qualify as a *document produced by a computer* and therefore admissible under Section 65?;

- just as with the difficulty that we have with any attempts to stretch the application of Section 65 to accommodate electronic transactions generated through electronic communications as expressed immediately above, we also have the same issues and difficulties with attempts to stretch Section 66 of the *Evidence Act* (proof of computer statements) to include all types of electronic communications. Obviously, if the electronic communication related to an electronic transaction is not printed as a computer statement, but remains in its electronic form either on the internet or on a website, than it is clear that such would be clearly outside of the scope of Section 66 of the Act;
- electronic communications and electronic records as generally discussed in Chapter 4 do present intrinsically separate and specific issues to the law of evidence concerning their admissibility and proof – away from the paper and ink generated documents and records. Therefore, we are of the opinion that a separate legal regime may have to be contemplated based on the various UNCITRAL Model Laws and laws of the other countries of similar legal systems, and
- as a consequence of this point, we propose that a separate legal regime may have to be established through these reforms to facilitate for the recognition and acceptance of electronic signatures based on the various UNCITRAL Model Laws as discussed in Chapter 4 of this paper .

5.2 NCD Preliminary Consultations and Views and Comments

For purposes of compiling this Draft Report we conducted preliminary consultations within the National Capital District (NCD) in May 2008. During these consultations (with relevant stakeholders), the issue of reforms to the *Evidence Act* to cater for these new developments was raised. Most people expressed the view that it is about time our country revised its current *Evidence Act* to permit the proof of Business and Electronic Records. The following are some of the arguments put forward:

- (1) to cover new computer and digital technology;

- (2) the aspects of admissibility of electronic records as evidence must be addressed, as electronic images can be altered or edited to reflect incorrect statements and images. Where there is hard copy as (secure) back up, this would begin to counter changes to otherwise solely electronic records. Reference to the use of firewalls and data security programs should be included to ensure that data are unadulterated. Secure data back – up systems in several locations should occur;
- (3) in this day and age electronic revolution is taking place at a faster pace and therefore the law of evidence needed to be reviewed and amended to cater for such;
- 4) model laws from other jurisdictions need to be looked at closely and also what type of technologies are being introduced to be defined as business records, Electronic Records and Electronic Communications;
- (5) in the past there was no email. Today we have email. The question then is does evidence constitute password as admissible in a court of law. Second, bank card PIN number, which is known only to one person and the fact that no one knows about it raises questions about its admissibility in a court of law; and
- (6) if other countries have done it, we will obviously come to use electronic records as evidence.

There is a need to ensure that provision is made for the legal recognition of electronic records and to facilitate the admission of such records into evidence in legal proceedings. As stated above, we are of the view that the provisions in the current *Evidence Act* (Sections 65 and 66) which provide for the admission and proof of computer generated statements and information, do not adequately provide for the admission and proof of the electronic records and electronic communication. Tape recording of evidence, may also be categorized as electronic record. New generation mobile phones that have an email/internet capacity can also be used to create electronic record, as well as through text messaging. There are many voice recording devices as well as telephone voice mail that can produce electronic record. It is presumed that electronic record can be written or printed out as video tapes, CD ROMS, DVD and hard copy. Sound recordings can also be "edited" and reproduced, as can composite devised images on the computer. Scanned and photocopied documents can become electronic records. New telephone equipment that has an internet facility

may likewise too. Video cameras, CCTV, and electronic surveillance cameras/equipment produce digital evidence are also in electronic form.

Most of the stakeholders we consulted stressed that our legislation has not kept up with modern technology and software systems. However, current law practice incorporates modern process as far as associated legislation allows relating to aspects of copyright, intellectual property rights, ownership of legal rights, or title. They further argued that there is a need for legal recognition of electronic records because:

- (1) The process of interpretation, admissibility proof and weighting need to be adjusted to reflect technological changes. The processes of establishing authenticity and of the electronic record for purposes of admission as evidence with regard to accuracy and weight of evidence is paramount;
- (2) there is a need to define what devices: computers, videos, DVDs, CDs, mobile phones as acceptable mediums for presenting acceptable (by laws) evidence that is considered legally reliable. Most businesses have access to such equipment and could provide records electronically. There may be a need to authenticate a scanned original document on occasion to avoid concealment or misrepresentation of facts. Changes to acceptance of a wider range of electronic record would avoid massive print files in court presentations;
- (3) in relation to photographic and machine reproductions or electronic images, our *Evidence Act* must reflect current technologies such as colour photocopies, scanners, video cameras, digital cameras, and other equipment capable of high resolution images and copies; and
- (4) the aspect of data security is not addressed, including penalties for falsifying documents, illegal alteration of original electronic documentation.

Submission and Consultations

During the national consultations, the majority of those consulted were of the view that the laws of evidence can and should be modified to permit the proof of business and electronic records by expanding the definition of document. Mr Daniel Kaima, a lawyer with Centre for Environmental Law and Community Rights submitted that the definition of the term ‘document’ in the Act should be widened to increase the scope of the law to admit

contents of documents into evidence in any accepted form, including those created through electronic mediums over time. After having observed the provisions in Division 5 Part IV of the Act it appears that these provisions are wide enough to cover records of electronic transactions. It would appear that merely introducing the rebuttable presumptions would effectively minimize the time and effort a proponent would go through meeting all the applicable requirements of the provisions in Division 5 of Part IV of the Act. The effect of introducing these presumptions would be a shift in the burden to a respondent to adduce evidence to rebut these presumptions in a given case. It is proposed that the definition of electronic communication in the Model Law on Electronic Commerce be adopted under an introduced legislation to give effect to electronic transactions in this jurisdiction. Such a definition will provide the basis not only to take account of current and perceived advances in the mediums in which electronic communication is facilitated and recognized, but lays the premise for records of electronic communication to be subject to pertinent laws of evidence for admissibility purposes.

CLRC Views

The CLRC is of the view that the law of evidence should be modified to cater for proof of business, electronic records, and electronic communication. On the other hand, electronic communication should be provided for under a separate legislation as proposed earlier. The legislation will meet all the requirements as set by the Model Law on Electronic Communication, which the CLRC considers appropriate to adopt with adaptations to suit the circumstances prevailing in the country. The legislation will have the effect of providing a regulatory framework that recognizes the importance of the information economy to the future economic and social prosperity of Papua New Guinea, and facilitates the use of electronic transactions, and promotes business and community confidence in the use of electronic transactions, and enables business and the community to use electronic communications such as email in their dealings with government.

Appendix 1 Proposed Draft Legislation

THE INDEDPENDENT STATE OF PAPUA NEW GUINEA

A BILL

for

AN ACT

Entitled

Electronic Transaction Act 2012

BEING an Act to provide for any kind of information in the term of a data message to be used in the context of commercial activities

MADE by the National Parliament to come into operation in accordance with a notice in the National Gazette by the Head of State, acting with, and in accordance with the advice Minister.

PART I - ELECTRONIC COMMERCE IN GENERAL

1. Interpretation

In this Act, unless the contrary intention appears-

"Date message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy;

"Electronic data interchange (EDI) means the electronic transfer from computer to computer of information using an agreed standard to structure the information;

"Originator" of a data message means a person by whom, or on whose behalf, the data message purports to have been sent or generated prior to storage , if any, but it does not include a person acting as an intermediary with respect to that data message;

"Addressee" of a data message means a person who is intended by the originator or receive that data message, but does not include a person acting as an intermediary with respect to that data message;

"Intermediary" with respect to a particular date message, means a person who , on behalf of another person, sends, receives or stores that data ,message provides other services with respect to that date message;

"Information system" means a system for generating, sending, receiving, storing or otherwise processing data messages.

2. Variation by agreement

(1) As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of chapter III may be varied agreement.

(2) Paragraph (1) does not affect any right that may exist to modify by agreement any rule of law referred to in chapter II0

PART II - APPLICATION OF LEGAL REQUIREMENTS TO DATA MESSAGES

3. Legal recognition of data message

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

4. Incorporation by reference

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.

5. Writing

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.

(2) Sub-Section (1) applies whether the requirement therein is in the form of an obligation not being in writing.

(3) The provision of this article does not apply to the following:

6. Signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if:

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is a reliable as was appropriate for the purpose for which the data message was generated or

communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) The provisions of this article do not apply to the following:

7. Original

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

(2) Sub-Section (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

(3) For the purpose of Sub-section (1)(a):

(a) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arise in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

8. Admissibility and evident weight of data messages

(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 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 its 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 integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor.

9. Retention of data messages

(1) Where the law requires that certain documents, records, or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

(a) the information contain therein is accessible so as to be usable for subsequent reference; and

(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(2) An obligation to retain documents, records or information in accordance with Sub-section (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.

(3) A person may satisfy the requirement referred to in Sub-section (1) by using the services of any other person, provided that the conditions set forth in subparagraphs (a), (b), and (c) of Sub-section (1) are met.

PART III - COMMUNICATION OF DATA MESSAGES

10. Formation and validity of contracts

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by the means of data messages. Where a data messages is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

(2) The provision of this article does not apply to the following.

11. Recognition by parties of data messages

(1) As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

(2) The provisions of this article do not apply to the following:

12. Attribution of data messages

(1) A data message is that of the originator if it was sent by the originator itself.

(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:

(a) by a person who had the authority to act on behalf of the originator in respect of that data message, or

(b) by an information system programmed by, or on behalf of, the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is entitled to regard a data message as being that of the originator, and to act on that assumption, if:

(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose, or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enable that person to gain access to a method used by the originator to identify data messages as its own.

(4) Sub-Section (3) does not apply;

(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or

(b) in a case within Sub-section (3) (b), at any time when the addressee know or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on the assumption, then, as between the originator and the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption. Except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the message was a duplicate.

13. Acknowledgement of receipt

(1) Sub-section (2) and (4) of this article apply where, on or before sending a data message, or by means of that date message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by

(a) any communication by the addressee, automated or otherwise,

or

(b) any conduct of the addressee

sufficient to indicate to the originator that the data message has been received.

(3) Where the originator has stated that the data message is conditional on receipt of the acknowledged, the data message is treated as though it has never been sent, until the acknowledgment is received.

(4) Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledge must be received; and

(b) if the acknowledgement is not received within the time specified in subparagraph (a), may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.

(6) Where the received acknowledge states that the related message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

(7) Except in so far as it relates to the sending or receipt of the data message, this article is not intended to deal with the legal consequences that may flow either form the data message or from the acknowledge of its receipt.

14. Time and place of dispatch and receipt of data message

(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters and information system outside the control of the originator or of the person who sent the data message on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows;

(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:

(i) at the time when the data message enters the designated information system; or

(ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee.

(b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.

(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).

(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purpose of this sub-section:

(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business

(b) If the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.

PART IV - ELECTRONIC COMMERCE IN SPECIFIC AREAS.

15. Actions related to contracts of carriage of goods

Without derogating from the provisions of part one of this Law, this chapter applies to any action in connection with, or in pursuance of, a contract of carriage of goods, including but not limited to;

(a) (i) furnishing the marks, number, quantity or weight of goods;
(ii) stating or declaring the nature of value of goods
(iii) Issuing a receipt for goods
(iv) confirming that goods have been loaded

(b) (i) notifying a person of terms and conditions of the contract;
(ii) giving instructions to a carrier;

(c) (i) claiming delivery of goods;
(ii)authorizing release of goods;
(iii)giving notice of loss of, or damage to, goods;

(d) giving any other notice of statement in connection with the performance of the contract;

(e) under-taking to deliver goods to a named person or a person authorized to claim delivery;

(f) granting, acquiring, renouncing, surrendering, transferring or negotiating rights in goods, and

(g) acquiring or transferring rights and obligations under the contract.

16. Transport documents

(1) Subject to sub-section (3), where the law requires that any action referred to in article 16 be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data messages.

(2) Sub-section (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for failing either to carry out the action in writing or to use a paper document.

(3) If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique.

(4) For the purpose of sub-section (3), the standard of reliability required shall be assessed in the light of the purpose for which the right or obligation was conveyed and in the light of all the circumstances, including any relevant agreement.

(5) Where one or more data messages are used to effect any action in sub-sections (f) and (g) of article 16, no paper document used to effect any such action is valid unless the use of data message has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of data messages by paper documents shall not affect the rights or obligations of the parties involved.

(6) If a rule of law is compulsorily applicable to a contract of carriage of goods which is in, or is evidenced by, a paper document, that rule shall not be inapplicable to such a contract of carriage of goods which is evidenced by one or more data messages or messages instead of by a paper document .