EVIDENCE DIGITALISED!

B.P. Gamarachchi

Head of Finance
Lanka Industrial Estates Ltd

1. Introduction

As a close acquaintance recently pointed out over a cup of tea, ever since the human being started using the ax,[1] supposedly the first machine ever,[2] technology has had an enormous yet undeniable impact on the life-style of human beings, for over thousands and thousands of years, if not millions! Moving forward, one would tend to agree that today we live in an era of digital miracles where technology appears to embrace our lives, to which more often than not, we are quite oblivious. It touches our lives even before we are born and refuses to leave its trail even long after our departure. Extent to which it affects our day-to-day living is vividly depicted in the following text.

"…ten years ago, if I went for a jog, any and all information relating to that jog would evaporate as soon as it happened. It would go un-captured. Now, that information is not only preserved…it gets uploaded to the cloud and propagated across my social networks…"[3]

In contrast, today, even the Government of Sri Lanka (GOSL) is very eager to enter into digital methods of handling payments with a view to enabling and facilitating electronic commerce or digital commerce. It is reported that *"GOSL is to set up a National Payment Platform"*[4] (NPP) in this connection where once established *"…all licensed commercial banks will be able to integrate with the NPP"*[5] which is to be supervised by the Central Bank of Sri Lanka through its clearing arm Lanka Clear Pvt. Ltd. Thus, it is apparent that banks and other financial intermediaries will be called upon to play a pivotal, enhanced role in the proliferation of digital commerce.

As far back as 2004, it was reported in a reputed financial journal that *"…the legal framework of a country contributes to the development and stability of its financial sector…by reducing legal uncertainties and risks and facilitating the orderly development of this sector.*[6] *"Computers…"* on the other hand are *"…an integral part of banking business."*[7] Fast forward the clock by a decade; this landscape has not altered itself dramatically in spite of various measures taken by the successive legislatures to combat this all important issue. It will not be an exaggeration to observe that the legislative enactments governing digital technology are still in its infancy world over. Now the Million Dollar question is as to how the law enforcement authorities and policy makers would embattle threats and risks posed by the advent of digital technology.

In this short article, the author attempts to analyze as to how the Law of Evidence and other laws in this respect have evolved over the years *vis-à-vis* the analogue and digital technological revolutions, with particular reference to the law relating to banking and finance.

2. History of computers

A study of the history of computing reveals the boundless ingenuity and capacity of the human brain. Nevertheless, researches and writers hold diverse views on the origin and chronological evolution of computers. We need to go back in history to 2400 B.C. to the era of the first known computing device of Babylonian origin called "Abacus" which is still in use in some parts of China. Next noteworthy effort came in the form of "Napier's Bones," an invention of the famous Scottish mathematician and physicist John Napier who is also credited with inventing "Logarithms." This was, in essence, *"an Abacus like device that greatly aided complex calculations involving multiplications and divisions."*[8] The Slide Rule introduced by William Oughtred and Wilhelm Shikard's mechanical adding machine are two other useful devices that made that presence felt.

Blaise Pascal, the French mathematician, invented a device similar to that of Shikard which is known as the "Pascaline." In 1673, the German mathematician Gottfried Leibniz introduced a more advanced mechanical calculator which was known as the "Step Reckoner." In the early nineteenth century, Joseph-Marie Jacquard developed a pattern weaving machine which is considered to be the first system of punched card data processing.

Around 1823, Charles Babbage, widely regarded as the father of the computer, demonstrated a simple operational model of his "Difference Engine." Though this was a failure, by about 1834, he was able to perfect a more general design called the "Analytical Engine." American born Herman Hollerith designed the first method of data storing in punched cards which could then be processed mechanically*."His system was used in 1890 by United States Census enabling it to accomplish the task months ahead at a much lower budget."*[9] Hollerith, then, went onto found the "International Business Machines Corporation" (I.B.M.).

Interestingly, World War II also contributed to the development of computing devices. Colossus, the first ever electronic digital computer with programmable capability was intensively used to break the then hostile German army's code known as Enigma.

Computers built up to that time were categorized as analog machines as they relied on mechanical sources of power or at the most a hybrid of mechanical and electrical power. The first substantial computer ENIAC (*Electrical Numerical Integrator and Calculator*) jointly "*developed by Presper Ekert and John Mauchly"* [10] heralded the dawn of the First Generation of Computers." These electronic valve (vacuum tube) intensive machines, which could be handled only by experts of computing with a high degree of patience and specific knowledge of programming in assembly languages, knelt the death sentence for analog computers used hitherto.

Gigantic machines of this era were very inefficient, thereby, compelling continuous research for more reliable, efficient means of computing. The transistor became a substitute for the vacuum tube which resulted in the second generation of computers. "*Second generation machines used more user friendly programs such as COBOL (Commercial All Purpose Symbolic Instruction Code), FORTRAN etc."*[11] In addition to demanding highly trained programmers, these machines which ran on transistors, too, had their intrinsic problems such as complex soldering, thereby leading to the invention of integrated circuits. (IC)

This brings us to the dawn of the third generation computers.

Third generation witnessed a veritable explosion in the use of computers. by and large. IC or the microchip led the world to the microprocessors such as "INTEL." Key differentiation of this generation was the convenient use of key boards, monitors etc which brought user interface within reach of people with relatively low levels of information communication technology (ICT) capability.

To this end, "APPLE II," a machine run mainly on BASIC (*Beginners All Purpose Symbolic Instruction Code*) was introduced at a much cheaper affordable price in the mid-seventies. Radio Shack introduced TRS-80 which was a popular home computer at the time (1977). Not to be outdone, *"IBM, too, has decided to get into the act and introduced IBM PC for the home computer market.*[12]Subsequently towards mid-eighties, "*… MACINTOSH, the first machine to use graphical user interface (GUI) was released making it more useful and convenient for the home computer segment.IBM counterattacked with machines supported by software such as LOTUS 1-2-3, Microsoft Word etc"*[13]

There is discernible overlap between third and fourth generation computers. These machines used very large scale integration (VLSI) with the aid of many thousands of integrated circuits built into a single silicon chip. "*… 'A NeXT' computer and its object oriented development tools and libraries were used to develop the world's first web-browser software and also to write the first web-browser, "World Wide Web (WWW)"*[14]

With the fifth generation machines, we speak of Artificial Intelligence where a machine will be programmed *to "act on its own volition according to situations present, learning and selforganization."*[15] Voice recognition is one such means that we are quite familiar with. Google's initiative of driver-less cars, known as Google Chauffer, is another. Thus, it is apt to state that *"Quantum computation, molecular and nano-technology will radically determine the future of computer technology and thereby the human life styles."*[16]

- Advent of the Internet and Electronic Mail

Invention of the Internet and electronic mail brought new vistas to the world of tech-savvy individuals. "*The Internet is the global system of interconnected* computer networks that use the

Internet protocol suite (TCP/IP) to link billions of devices worldwide."17 These inter-linked computers could range from domestic personal computers, mobile devices such as smartphones to highly secure complex machines stationed in places such as "NASA" at the extreme end. Electronic mail, on the other hand, is a method of exchanging digital messages between computer users. This can be deployed internally in an organization using its customized Intranet (a restricted from of Internet) or with the global population through the Internet."*E-mail (electronic mail)"* is, thus, defined *"as the exchange of computer-stored messages by telecommunication."*[18]

- ANALOGUE vs DIGITAL

An avid, observant reader, by now, would have visualized the contrasting nature and mechanisms involved in the two methodologies, viz, analogue and digital. Avoiding the intricacies of technical jargon, in basic layman's terms, an analog computer is a machine that derives its power from mechanical or electrical sources whereas a digital computer is an equipment which operates with numbers expressed directly as digits that is only zero and one for all its complexity. This is also commonly referred to as the binary language.

Nonetheless, for the purposes of completeness and academic credentials, it may be opportune now to examine some of the widely respected definitions of the two. Firstly, it may be recalled that almost all of the computing devices of olden days, particularly during the period leading to the nineteen-fifties were analog machines which used mechanical methods as means of sourcing power.

Wikipedia, thus, states that *"An analog computer is a form of computer that uses the continuously changeable aspects of physical phenomena such as electrical, mechanical, or hydraulic quantities to model the problem being solved. In contrast, digital computers represent varying quantities symbolically, as their numerical values change."*[19]

Similarly, a digital computer could be defined as *"a computer that performs calculations and logical operations with quantities represented as digits, usually in the binary number system."*[20]

3. Law of evidence

Importance of evidence in any form of legal proceeding cannot be underestimated whether it be a civil suit involving civilians such as individuals, legal persons in the capacity of the Attorney General, duly incorporated corporate bodies etc or whether it is a criminal proceeding where the State to prosecutes various perpetrators of offences committed against the State. Once a particular issue or an action is instituted in a competent Court of Law, for a decision, it is the duty and the responsibility of the relevant court to deal with it according to the procedure established by Law, in delivering its judgment. In doing so, the Judge will intensely rely on the relevancy and

admissibility of evidence submitted to him. He will form an opinion, based on the evidence adduced as to the events that would have occurred.

It is important to observe that in the case of a criminal matter, the prosecution is required to prove its case beyond any reasonable doubt whereas in civil litigation, the degree of burden of proof is limited only to the extent of balance of probability. Thus, the major factor influencing the final judgment would be the relevance, admissibility and the truthfulness of the evidence placed before the Court by the two competing parties. Nonetheless, "*Stephen (1872: 3–4, 6–7) long ago noted that legal usage of the term "evidence" is ambiguous. It sometimes refers to that which is adduced by a party at the trial as a means of establishing factual claims."*[21]

Let us now examine some of the popular definitions of Evidence. Jeremy Bentham, the renowned English philosopher and jurist chose to state "a*ny matter of fact, the effect, tendency, or design of which, when presented to the mind, is to produce a persuasion affirmative or disaffirmative concerning the existence of such other matter of fact."* [22]

Different writers have attributed more comprehensive and purposeful meanings. Our own Evidence Ordinance of 1895 is a masterpiece of legal draftsmanship for it has robustly withstood the test of time. *"It is unique and the only one of its kind ever gained so much recognition for its precision and terseness"*[23]and is in a genre of its own.

The Ordinance reckons:

"Evidence" means and includes—

(a) all statements which the court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry: such statements are called oral evidence:

(b) all documents produced for the inspection of the court; such documents are called documentary evidence."[24]

The statute, therefore, recognizes and categorizes evidence into two as follows:

Oral Evidence;
Documentary Evidence.

As such, "*Oral Evidence must, in all cases' whatever be direct; …*" [25] Succinctly put, if it refers to a fact which could be seen, then, it must have been seen by the person giving evidence. Similarly, if it applies to situations of a fact which could be heard or perceived by senses, then, the witness himself must have heard or perceived it. On the other hand, *"Document" means any matter expressed or described upon any substance by means of letters, figures, or marks or by more than one of those means, intended to be used, for the purpose of recording that matter*." [26]

In general Hear-say Evidence is not admissible in the judicial system of this country even though there are few exceptional circumstances which prevail. In other words, evidence should be in its original form. This was widely discussed in "*Subramaniam vs. the DPP*."

"*Evidence of a statement made to a witness by a person who was not himself called as a witness might or might not be hearsay. It was hearsay and inadmissible when the object of the evidence was to establish the truth of what was contained in the statement. It was not hearsay and was admissible when it was proposed to establish by the evidence, not the truth of the statement but the fact it was not made."*[27]

Now, a question might linger in the mind of the reader with regard to the production of "objects" (which is known in Sinhala as "□□□ □□□□□") as the statute is silent on the matter. However, Section 60 (second proviso) sheds some light into the matter.

"...provided also that, if oral evidence refers to the existence or condition of any material thing other than a document, that court may, if it thinks fit, require the production of such material thing for its inspection"[28] This is referred to as "Real Evidence" in the legal parlance.

Therefore, *"In summary, at least four possible conceptions of legal evidence are in currency: as an object of sensory evidence, as a fact, as an inferential premise and as that which counts as evidence in law. The sense in which the term "evidence" is being used is seldom made explicit in legal discourse although the intended meaning will often be clear from the context*." [29]

4. How the law evolved over the years

Sir Francis Bacon (1561-1626), the famous English philosopher and Attorney General of UK, once quipped *"He that will not apply new remedies must expect new evils; for time is the greatest innovator*." [30]In other words, world has little choice in a matter of innovation as every-one of us is compelled to embrace such technological advancements sooner or later. In the present context, researchers intensely focus on artificial intelligence techniques such as hands free communication, voice recognition and further, neural networks, nano-technology, virtual reality, Internet of Things, 3-D printing etc. "*…Virtual reality, for instance, will soon be creating an environment that will help you meet a client (and many others) while seated in different locations..."*[31]

Financial institutions were at the forefront of commercial exploitation of digital innovations in order to garner the best benefits that emerged in terms of efficiency, speed, accuracy, competitive edge, ability to handle large volumes etc. Competition looms large in this highly regulated market where there are more players than what the market can comfortably absorb. In the so called global village, technology has been challenging the status quo of the financial services industry where the traditional "brick and mortar" structures are under tremendous pressure, though many argue that it will not fade away in the near future. On the other side of the story is

the number of inroads made by the Telecommunications Services Providers and software developers affectionately dubbed as "Fin-tech" companies into areas which were once acknowledged as the invincible domain of financial intermediaries. Chinese electronic commerce giant "Alibaba" which is omnipresent, challenging even the likes of "Amazon.com" is one such candidate. This compelled the industry to seek new business strategies to avoid erosion of business volumes, by relegating themselves even to the extent of forging strategic alliances with the telecommunications giants. Thus, digitalization of the financial services industry has become mandatory rather than obligatory for the institutions not only for mere survival but also to budge ahead of competition.

Nonetheless, mere embracing and adoption of digital technology is not a panacea for all ills. One of the biggest challenges that the law-makers as well as the users are confronted in this respect is to keep abreast with the new developments in computer technology, particularly with the advent of digital era. Up until about 1995, Sri Lanka maintained a rather lackadaisical approach to combating such issues as was observed in the case of "*Benwell vs. The Republic of Sri Lanka."*[32]

A brief description of the facts of the case as follows;

"On 27.11.1978, P. G. J. Benwell was arrested on a warrant issued by the High Court of Colombo, under the provisions of Extradition Law, No. 8 of 1977, in pursuance of a request made on behalf of the Government of Australia, to extradite Benwell from Sri Lanka to Australia as he was accused of certain criminal offences.

During the proceedings, the Court of Appeal observed that the evidence adduced by the prosecution by way of computer print outs were not acceptable in terms of Section 34 of the Evidence Ordinance.[33] *Under that, the word 'book' signifies a collection of sheets of paper bound together with the intention that such binding shall be permanent and the papers used collectively in one volume. Court then proceeded on the basis of Section 100 of the Ordinance*, [34] *to look to the law of England which can be brought in.*

In England under the Civil Evidence Act, 1968, computer evidence has been made admissible only in civil cases and that too under the most stringent conditions. One of these conditions is that throughout the material part of the relevant period the computer was operating properly." [35]

On the basis of these arguments, the request for extradition has failed and the Court held, inter alia, *"… (2) Computer evidence is in a category of its own. It is neither original evidence nor derivative evidence. Under the law of Sri Lanka, computer evidence is not admissible under Section 34 of the Evidence Ordinance nor under any other section of the Evidence Ordinance*." [36]

However, to the credit of the Judicial System of Sri Lanka, it has displayed a sufficient degree of innovation and flexibility in interpreting the existing provisions of the Evidence Ordinance. Cases such as *"Abubaker vs. The Queen"*[37](where a tape recording of a political speech made was accepted as Evidence under the provisions of Section 60 of the Ordinance), "*Kularatne vs The*

Queen, (telephone conversation was admitted as evidence in terms of Evidence Ordinance Section 3), "*Kularatne vs Rajapakse*,"[38] Re. in the "*Trial of S. A. Wickremasinghe"*[39] (where the recording of a telephone conversation was accepted as evidence*) s*tand as testimony to this fact.

Even in the United Kingdom, there had been several instances where the judiciary exercised some degree of freedom and flexibility in interpreting the existing law in order to accommodate certain available evidence. In *"Kajala vs. Noble*, it *appears to have been assumed that the policy of the BBC in insisting on retaining the original of their films precluded production of the originals so as to render the video-cassette copy admissible as admissible evidence..."*[40]

In "*R vs. Dodson and Williams (1984)," two men were involved in an attempted armed robbery… There were no available witnesses who knew the defendant. There were photographs available to be placed before the jury taken from security cameras. The case demonstrates that it is permissible for the Crown to place before a jury photographs taken by a security camera and then to invite the jury to conclude"*[41] In "*Castle vs. Cross (1984), First-hand evidence, in this case, a print-out from a device, of what is displayed or recorded on a mechanical measuring device is real evidence, admissible at common law*."[42]

However, in cases such as "*R. vs. Preddy"*[43] apparent reluctance was discernible on the part of English judiciary to accept computer evidence based on the provisions of their (then) statutes. In *"R v Gold and Schifreen"[1988]*,[44] a password failed to be categorized as a physical device. (i.e. real evidence)

5. Evidence ordinance amended

"All the textbooks on electronic evidence and e-discovery appear to agree on one area. Digital evidence is one of the great, if not the greatest, challenges facing the civil (and criminal) litigation."[45]Similarly even in Sri Lanka, by about the mid-nineties, there had been a considerable degree of awareness and intellectual capacity amongst the legislators, the judiciary and other scholars regarding the relevance and undeniable application of computer based evidence. This was substantiated by factors such as;

√ that computer based evidence was in essence in conflict with the "hear-say evidence rule**"** because very often the entire process of producing a computer print-out or such an output involves a large number of live-ware (human beings) thus bringing in a semblance of "hear-say" evidence to the case which makes it in admissible in a court of law;

√ that data in a computer cannot be considered documentary evidence in terms of Section 3 of the Evidence Ordinance and to ensure its evidentiary value certain specific changes to the existing law had to be incorporated;

√ that this type of evidence including audio-visual recordings lacked the capacity to be perceived by senses as required in Section 60 of the Evidence Ordinance. This hurdle had to be overcome before such evidence is made admissible in a proceeding.

This scenario paved the way for the Evidence (Special Provisions) Act, No 14 of 1995.[46] This Act, has, to a great extent, filled a *lacuna* that existed hitherto in relation to the computer based evidence enabling the admissibility of contemporaneous recordings and reproductions thereof in civil and criminal proceedings.

Let us now examine some of the more important Sections of the Act.

Interpretations given in Section 12 of the Act are;

"In this Act unless the context otherwise requires-

- "computer" means any device the functions of which includes the storing and processing of information;

- *"duplicate" means a counterpart, produced by the same impression as the original, or from the same matrix or by means of photography (including enlargements, reductions, and miniatures), or by electronic, mechanical or chemical reproduction or re-recording, or by other equivalent techniques which accurately reproduces the original;*[47]

It also interprets terms such as the "original" and the ''statement."

According to the provisions of the Act, a contemporaneous recording or re-production thereof will be admissible as evidence in spite of being in conflict with "Hear-say" evidence rule. A recording, whether it be audio, video or filming, as long as it is carried out simultaneously as the incident occurs, is termed contemporaneous.

Section 4, thus, states,

(1) In any proceeding where direct oral evidence of a fact would be admissible, any contemporaneous recording, reproduction thereof, tending to establish that fact shall be admissible as evidence of that fact, if it is shown that – fact If;

(a). the recording or reproduction was made by the use of electronic or mechanical means;ubject to subsection (3) of this section, the recording or reproduction is capable of being played, replayed, displayed or reproduced in such a manner as to make it capable of being perceived by the senses;

(b). at all times material to the making of the recording or reproduction, the machine or device used in making the recording or reproduction, as the case may be, was operating properly, or if it was not, any respect in which it was not operating properly or out of operation, was not of such a nature as to affect the accuracy of the recording or reproduction;

(c). the recording or reproduction was not altered or tampered with in any manner whatsoever during or after the making of such recording or reproduction, or that it was kept in safe custody at all material times , during or after the making of such recording or reproduction and that sufficient precautions were taken to prevent the possibility of such recording or reproduction being altered or tampered with, during the period in which it was in such custody"[48]

It is, therefore, necessary that four basic conditions be fulfilled for this kind of evidence to be admitted, viz.,:

a. Use of electrical or mechanical methods for the recording/reproduction
b. Should be used in a such a manner that it can be grasped by senses
c. Must have been in proper use and if not the defect should not be of any materiality
d. Recording/reproduction should be in its original form in safe custody without being tampered with
e. Contemporaneous recording/reproduction is preceded by admissible oral evidence

Subsection (2): "If the conditions set out in subsection (1) are satisfied, the recording or reproduction shall be admissible in evidence or the fact recorded or reproduced , whether or not such fact was witnessed by any person"[49]

According to sub - section 3 of the Act, if the aforesaid conditions are fulfilled, even a transcript, a translation or at least a transformation of such recording/reproduction could be made admissible. Section 4, further provides that whether there was the involvement of one or more machines or devices or a combination of machines, such recording/reproduction could be made admissible.

The Act further provides that the live-ware (human beings) involved in the process are not required to be present in person in a Court to testify, instead an affidavit duly signed by them[50] will suffice. The Act supplemented the computer based evidence with wide ranging powers and flexibility, despite the strong possibility of manipulation in the hands of an unscrupulous character. There is, of course, the necessity that the recording must be in its original form. *"... the attitude of our courts in regard to such matters have generally been permissive rather than prohibitive..."*[51] Substantial deviations from time honoured practices such as the Rule of Best Evidence, rejection of Hear-say evidence, admissibility of only the Oral and Documentary Evidence etc have been witnessed under these sweeping changes.

6. Other relevant statutes

Though the above Act could be considered a remarkable improvement over the status quo that existed, it still contained a considerable quantum of shortcomings and gaps forcing the authorities to a relentless search for the furtherance of law in this regard. Recent scandalous

release of a video clip to the wide world of internet, causing severe reputational damage to a well-known institution, for no fault of theirs, is a classic example of this danger. To compound of matters further, affected institution would be unable to take any action due to potential failure on account of admissibility of evidence. Intricacies of the issue were further substantiated, in another incident when a leading politician made some apathetic remarks leading to possible compromise of the sovereignty of the country. In the ensuing proceedings, it transpired that the particular television company which is purported to have telecast the speech was unable to produce the original video as the equipment containing it has been already re-used for a subsequent recording. Alas, that brings about an abrupt end to the matter.

♦ ELECTRONIC TRANSACTIONS ACT, No. 19 of 2006

One of the biggest challenges of the modern era was the facilitation of digital and electronic commerce, especially because it involves cross border transactions, culminating in coercion in areas of jurisdiction as well as the ambit of basic laws of the international community commonly referred to as International Law. *"It is perhaps in this light that United Nations Commission on International Trade Law (UN ICITRAL) introduced a model Law which proposes ways and means of executing electronic transactions in an expedient and legally acceptable manner. An important feature of the model is the acceptance of electronic data storage and acceptance of such data as evidence in dispute resolution."* [52]

Sri Lanka, in another exhibition of trend-setting in the SAARC region, has adopted this UN ICITRAL model based law, thereby, introducing ways and means of executing electronic transactions in an expedient, legally compliant manner, for data interchange and also for accepting and facilitating such transactions; also to establish an authority for recognition of Electronic Signatures and Certification Service Providers who could assist in ascertaining confidentiality, authenticity and integrity of electronic data. Further, it aims to dispel doubts and myths about electronic transactions. The statute, Electronic Transactions Act, No 19 of 2006[53] also encourages the use of reliable forms of electronic commerce and strengthens the growth of electronic commerce in the country.

The objectives of the Act are as follows

- "facilitate domestic and international electronic commerce by eliminating legal barriers to establishing legal certainty
- to encourage the use of reliable forms of electronic commerce
- to facilitate electronic filing of documents with government and to promote efficient delivery of government services by means of reliable forms of electronic communication
- to promote public confidence in the authenticity, integrity in electronic commerce and
- *reliability of data message*, *electronic documents*, *electronic records or other communications…"*[54]

Heralding a clear and distinct message that Sri Lanka is desirous of being at the forefront of innovation and accordingly the country should embrace and introduce modern legislation in the field of commerce and industry, the lawmakers under Section 21 of the Act, provided

"Any information contained in a data message, or any electronic document, electronic record or other communication –

a. touching any fact in issue or relevant fact; and
b. compiled , received or obtained during the course of any business, trade or profession or other regularly conducted activity, *shall be admissible in any proceedings…" "Section 21: sub-section (2):*

Nothing contained in the Evidence (Special Provisions) Act, No. 14 of 1995 shall apply to and in relation to any data message, electronic document, electronic record or other document to which the provisions of this Act applies. [55] *(Section 22:)*

Earlier the Evidence (Special Provisions) Act, No 14 of 1995 enabled the acceptance of electronic and computer evidence as admissible in a dispute before a court of law. However, with the introduction of Section 22 (as above), the significance and relevance of the said Special Provisions Act was drastically diluted.

First meaningful interpretation and test of this Act was observed in the money recovery case of "*Marine Star (Pvt) Ltd. Vs. Amanda Foods Lanka (Pvt) Ltd*"[56] when Justice K. T. Chitrasiri of the Commercial High Court of Colombo accepted Short Message Services (SMS) as valid evidence before a Court of law. In this case the plaintiff company produced before the Court, photocopies of several SMSs sent by the defendant company, to prove the liability of the defendant. Despite objections raised by the Counsel for the Defendant, after a careful consideration of the matter, Justice Chitrasiri delivered his judgment justifying the reasons for admitting SMSs as valid evidence in law. *"As it concerned an important issue on rules of evidence, especially at a time when there is a rapid development in technology taking place, Court decided to consider the issue carefully",* the judgment states.[57]

This judgment could be commended for making an effort to achieve the stated objectives of the Act whilst also undertaking an in-depth study of Evidence Ordinance and the Evidence (Special Provisions) Act, No 14 of 1995. It has been welcomed by a number of scholars in the legal field as well as by the general public.

"It is my opinion that a short message commonly described as SMS falls within the scope of the Electronic Transactions Act and therefore the evidence sought to be produced by the plaintiff could easily be admitted in evidence under Section 21 of the said Act No. 19 of 2006" [58] observed, Justice Chitrasiri.

♦ COMPUTER CRIMES ACT, No 24 of 2007

This statute supplements the above Act in investigating payment card frauds related to electronic payment systems. It enabled the identification of computer crimes and facilitation of legal action in respect of computer crimes and matters incidental to it.

Certain provisions of the statute impose criminal liability on various computer related activities and therefore are of critical importance.

Every offence under this Act shall be a cognizable offence within the meaning of, and for the purpose of, the Code of Criminal Procedure Act, No. 15 of 1979.- (Section 16)

Accordingly, the following activities are designated as offences in the Act;

- Securing unauthorized access to a computer (Section 3 - Marginal Note)
- Doing any act to secure unauthorized access in order to commit an offence
- Causing a computer to perform a function without lawful authority
- Offences committed against national security the national economy ; or public order
- Dealing with data sales, purchases & down-loading , unlawfully obtained data
- Illegal interception of data
- Using of illegal devices
- Unauthorised disclosure of information enabling access to a service

(the above points are based on the marginal notes of Sections 3 to 10 of the Act)…"[59]

Even an attempt to commit or abetting or conspiring to commit these offences could attract criminal liability. The Act also carries a comprehensive list of interpretations. Incidentally, the term computer carries almost identical definition and is consistent with the provisions of other statutes dealing with related subjects.

♦ PAYMENT DEVICES FRAUDS ACT, No. 30 of 2006

This Act aims to deal with offences connected with the possession or use of unauthorized payment devices and to protect persons lawfully issuing and using such payment devices.

♦ SRI LANKA TELECOMMUNICATIONS ACT, No 25 of 1991

"*Intrusion, interception and disclosure of contents of a message by anyone including telecommunications officials, other than in the course of their duty, is an offence as per Sections 52-54 of the Act.*"[60]

♦ **EVIDENCE SPECIAL PROVISIONS ACT, No 32 of 1999**

According to Section 4 of this Act, in the proceedings for an offence concerning child abuse, a video recording of a preliminary interview between the affected child and an adult (other than the accused) is admissible as evidence under certain conditions.

♦ **Absence of a Data Protection Act**

Sri Lanka is yet to introduce any legislation for the protection of data though the subject matter was widely discussed for almost two decades**.** Data protection is an issue of privacy and *"…if Sri Lanka is really willing to accept the benefits of globalization and getting absorbed into International Trade we still are not too late for any proposed data protection law that should be based on European model of the EU directive…"*[61]argues one scholar. It is thus high time that Sri Lanka enacted necessary legislation to protect data privacy and integrity rather than leaving them to the vagaries of market forces to determine.

7. Recent developments

The financial services industry has its own share of difficulties ranging from keeping pace with the technological developments to countering the threat of cyber-crime. It is the life blood of commerce and industry, world over, an unenviable position it has enjoyed over centuries.

Now, what are the challenges and trends we must deal with in the short to medium term?

New Trends

According to an article published in US NEWS recently, some of the trends that would affect the industry in relation to digital technology are a follows:

Fewer people will head to branches

"Mark Hamrick, senior economic analyst for Bankrate.com, says the number of Americans foregoing branch visits is on the rise." [62]

Apparently, this is true of Sri Lanka, too, in particular, with the advent of many mobile phone applications in addition to the intense promotion and use of internet banking by some banks, with little or no frills at all.

Digital and branch experience will merge

"As mobile services expand, banks will be looking for more ways to integrate banking on a phone with banking in a branch…" says Byron Vielehr, President of the Depository Institution

Services group for Fiserv, which provides technology solutions for banks and financial institutions….," Vielehr says. "For example, you may start an application online, realize you need help and then finish it at the branch."[63]

Again, in Sri Lanka, this facility is already in place where some banks permit the customer to open his account on line before heading to a pre-determined branch of his or her choice only to comply with the bare essentials of the regulatory process.

Branches will start to go digital.

"Mobile banking won't only be something for consumers in 2016. The banks themselves may start to use mobile technology in their branches." Vielehr says "some branches are "unshackling" tellers from the counter and giving them tablets so they can meet with customers more informally and comfortably either in the lobby or private offices. Other branches are adding technology by installing self-service kiosks or video ATMs that provide the opportunity to chat with a remote teller." Vielehr even tells of "one bank in Switzerland that has installed an automated safety deposit system that allows customers to check their deposit boxes without ever talking to a live person…" [64]

A golden opportunity is created for Sri Lankan counterparts to exploit!

Mobile payments will continue to make in-roads.

"Despite the onslaught of ads touting the benefits of services like Apple Pay or Android Pay, only 22 percent of mobile phone users made a mobile payment with their device in 2014, according to a Federal Reserve mobile financial services report last year. That could be changing in 2016." [65]

Sri Lanka, with the robustness of her relatively competent "fin-tech" companies are almost in line with this trend as some banks have joined hands with software developers in introducing innovative methods of carrying out transactions through the use of their own smart-phones , thereby, eliminating the hassle of visiting a branch.

Regional banks will get in on mobile deposits

"Before a few years ago, people thought they'd always have to go to branches to deal with checks," Vielehr says. "Now, people can simply snap a photo of their checque to have it instantly deposited, a service over half of mobile banking customers used in 2014, according to the Federal Reserve." [66]

This innovative proposition is readily available for the industry in Sri Lanka whereby they could eliminate the administrative burden of scanning the images of cheques deposited and conveniently transfer it to the customer.

Chip cards may finally see some action.

"Another technology that may finally be ready for prime-time is chip cards. While there was much ado about banks switching over to chip cards last year, you probably haven't noticed anything different in the checkout, even if you have a new card." [67]

Sri Lanka is yet to come to terms with "wi-fi" enabled chip cards or card insertion at the point of sales terminal which is a more secure feature available in technologically more advanced countries, even though there are strong signs of "tech-savvy" banks trying to introduce same.

Threat of cyber-crime – the "SWIFT" hack

Whilst these are some of the more encouraging developments for the industry to take note of, the more recent widely publicized hacking of the computer systems of the Central Bank of Bangladesh brings in new dimensions to the well-being of the industry. In early 2016, a bid to swindle the Federal Reserve Bank of USA (the fed) by some unknown cyber-criminals, to the tune of nearly U.S. $ 1.0 billion was thwarted, in the nick of time, by a sheer stroke of luck than by the vigilance of the system that was in place.

Obvious inertia was visible as a Reuter initiated examination has revealed : "…discussion with various parties show disarray and bungling at all financial institutions involved…" [68] Those errors envelope a cross section of banks commencing from the "fed" itself to Rizal Commercial Banking Corporation in the Philippines, via South-Asia where there is lot of finger-pointing and blame passing. While it is alleged that the Bangladeshi Bank lacked proper cyber-security systems in place, the FED was rather lethargic to react, it is reported and the bank in Philippines was found wanting for seriously compromising the basic tenets of account opening such as the KYC (Know Your Customer) rule. "…under the Philippine banking laws, the stolen funds could not be frozen until a criminal case was lodged..."[69] This apparently permitted the criminals to get away with their "hard earned heist."

The whole saga demonstrates how easy it is for a cyber criminal armed with appropriate technical know-how to carry out a huge heist of U.S. $ 81 million without even touching a firearm ever whilst brusquely revealing the inadequacy of the processes in place.

Other issues

Problems associated with cyber-crime and technological development could lead to unprecedented vistas of privilege and privacy as was experienced by APPLE Inc. and the general

public of USA. In the aftermath of the infamous San Bernardino (California) massacre, Federal Bureau of Investigations (FBI) demanded, on the basis of the All Writs Act,[70] that Apple Inc. crack the automatic security features of its operating system iOS9 so that FBI could investigate further the contents of an APPLE phone used by one of the criminals who died in the shooting. Apple vehemently resisted the move in the name of privacy, privilege and insecurity, citing that it could result in dire consequences subsequently. A major legal tangle was, anyway, averted when an Israeli based software company Cellebrite managed to break into the said phone at a cost of US $ 15,278.02.[71]

The highly respected and admired tech company from Cupertino argued on the basis of privacy, a fundamental right guaranteed in the First Amendment to the U.S. Constitution. "Being compelled to write new software for this purpose amounts to compelled speech which is a violation of the First Amendment…"[72] counter-argued Apple. This, nonetheless, is not the only occasion where tech companies came within the iron grip of the long arm of law, quite unfairly. The 1879 datelined act empowers US judiciary to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to usages and principles of law…"[73]

There are other cases such as US vs. New York Telephone Company[74] and "the Brooklyn cases"[75] originated under the purview of the statute while there are 76 other such case pending, as of March 2016. Another perspective that technological advancement could bring about, therefore, is the potential intrusion into our private lives. Every time an investment on a smart phone or any other internet enabled computer device is made, it exposes us to the wide world of internet through the IP (internet protocol) address of the apparatus, seriously jeopardizing individual privacy.

8. Conclusion

"Technology and technology related innovations play a significant role in our lives today. The computer, computer systems and the internet are almost household things.[76] Right through the planet earth, access to computers has become an integral part of day to day life of humans. As discussed earlier, every individual, every organization whether in the public or private sector has embraced the marvels and convenience of the digital revolution. However, on the flip side, it is critical to be aware that we live in such volatile times where there is intense discussions about human enhancements, implanting of brain chips, human genetic modifications that would eventually lead to "super humans" etc which will be a reality before long. This could, perhaps, spell destruction and irreversible damage to the world as history teaches us that in the hands of narrow minded, self-centered leaders, it could very well bring about irreversible damage to the human race.

One of the biggest challenges is that technology develops and expands at a rapid pace, with which the law-makers and policy think tanks find it hard to keep abreast. This lag effect often

becomes a serious impediment to the proper administration of justice. On the other hand, various scholars and regulators demand more stringent measures against failure to preserve and also to furnish electronic information, especially in the event of a cyber-crime. These proposals include, inter alia, substantial financial penalties (to act as a deterrent), contempt (of court) proceedings and also possible convictions as a criminal offence.

With the increasing possibility of technology reaching every nook and corner of the global village on a real-time basis with computer technology being ubiquitous, the role carved out for international agencies such as UN ICITRAL, WTO (World Trade Organization), Council of European Convention on Cybercrime (also known as the cyber crime convention), [78] would be to continue with the good work carried out hitherto whilst maintaining a constant vigil on possible vulnerabilities.

As the University of British Columbia states,

"The territory is huge, and the impact of the digital era on business and the practice of law cannot be measured easily. The more input the research receives, the better the odds that some refinements or even new strategies will emerge to help the courts and the legal profession." [79] and in the end the mankind!.

Reference

- https://www.superteacherworksheets.com/simple-machines pictures WMTNM.pdf accessed at 8.40hrs on 04 July 2016: "An ax is used to chop wood. The metal part chops through the wood, pushing it apart into two smaller sections. An ax uses its wedge effectively to separate the object into parts, by using its lateral force and movement.
- https://en.wikipedia.org/wiki/Machine accessed at 8.20hrs on 04 July 2016:"A machine is a tool containing one or more parts that uses energy to perform an intended action."
- "Inside APPLE's Code War"; TIME Magazine, 28 march 2016 pg 28 para 18
- "National Payment Platform for online payments to promote digital commerce," The Sunday Times, dated 17 July 2016, pg. 18
- ibid 4 above
- Somaratne, Inoka, "Legal Reforms for the Financial Sector in Sri Lanka"; Bankers Journal (Volume XXIII November 2004, pg. 74 para 2)
- Fernando, V.M., "Financial Innovation and the Use of ICT in the Banking Sector" The Professional Banker, June 2005,pg 18
- https://en.wikipedia.org/wiki/History_of_computing_hardware; accessed at 7.40am on 19 July 2016
- http://homepage.cs.uri..edu/faculty/wolfe/book/Readings/Reading03.htm accessed at 7.55am on 19 July 2016
- ibid 9 above
- ibid 8 above
- ibid 9 above
- ibid 8 above
- http://www.hptunotes.com/Includes/Notes/The%20Five%20Generations%20of%20Computer s.pdf accessed at 9.10am on 19 July 2016
- ibid 8 above
- ibid 14 above
- https://en.wikipedia.org/wiki/Internet accessed at 9.10am on 20 Jul 2016
- http://searchexchange.techtarget.com/definition/e-mail-electronic-mail-or-email accessed at 9.20am on 19 July 2016
- https://en.wikipedia.org/wiki/analog accessed at 9.40am 20 Jul 2016
- http://www.yourdictionary.com/digital-computer?print=preview accessed at 5.40am on 18 July 2016

- http://plato.stanford.edu/entries/evidence-legal/ accessed at 7.40am on 28 July 2016
- "The Works of Jeremy Bentham," Edinburgh; William Tait, 78, Princes Street pg 208 Year 1839
- Tilakaratne, Mahanama, "The Law of Evidence,", Samayawardhana Book Shop Pvt Ltd (2008)pg v
- Evidence Ordinance of Sri Lanka 1895 (Section 3)
- ibid 24 above Section 60
- ibid 24 above Section 3
- http://www.casebriefs.com/blog law/ evidence/ evidence-keyed-to-waltz/the-hearsay-rule/ subramaniam-v-publicprosecutor/ accessed at 5.30am on 19 August 2016 "Subramaniam vs. Public Prosecutor [1956] W.L.R. 965 I"
- ibid 24 above Section 60 second proviso
- ibid 21 above
- http://www.brainyquote.com/quotes/quotes/f/francisbac130602.html accessed at 5.40am on 23 July16
- "Sri Lanka's Future Lies in Tech Companies" The Sunday Times, Business Times, 31 July 2016, pg 2
- "Benwell vs. The Republic of Sri Lanka [1979](2) Sri NLR 194"
- ibid 24 above Section 34 – "entries in books of account, regularly kept in the course of business, are relevant…"
- ibid 24 above Section 100 - "what questions to be determined according to English Law of evidence"
- ibid 32 above
- ibid 32 above
- "Abubaker vs. The Queen,54 NLR 566"
- "Upali Dharmasiri Welaratne vs. Wesley Jayaraj Moraes, S.C. Appeal No.65/2003"
- "Re. in the trial of S.A. Wickremasinghe, 55NLR511"
- "Kajala v Noble (1982) 75 Cr App R 149 (19.3.3)"
- "R vs. Dodson and Williams (1984) 79 Cr.App. R. 220"
- http://swarb.co.uk/castle-v-cross-1984/ accessed at 5.30pmon 19 August 2016 "Castle vs Cross(1984)1 WLR 1372, [1985] 1 All ER 87":
- "R. vs Preddy (1196, 3AII ER 48)"
- "R v Gold and Schifreen [1988] 2 WLR 984"
- http://www.courthouselibrary.ca/training/stream/13-07-25/Law_of_Evidence _in_the _Digital_ Environment_ UBC_ study_ calls_ seeks lawyers _insights.aspx accessed at 1.30PM on 04 July 2016
- Evidence (Special Provisions) Act, No 14 of 1995
- ibid above Section 12
- ibid above Section 4 Subsection 1
- ibid above Section 4 Subsection 2
- ibid above Section 5
- ibid above 38
- Gamarachchi, B.P.,"*Volatility : Its Impact on Sustainability of Contractual Obligations*" Association of Professional Bankers – Anniversary Volume 2012
- Electronic Transactions Act, No 19 of 2006
- ibid 53 above Section 2
- ibid 53 above Section 21 and 22
- "Marine Star (Pvt) Ltd. vs Amanda Foods Lanka (Pvt) Ltd, HC(Civil)181-2007"
- *"Commercial High Court Judge Admits SMS as Evidence,"* The Nation, 17 August 2008
- ibid 57 above
- Computer Crimes Act, No. 24 of 2007, Sections 3 to 14 and 16
- Abeyratne, Sunil D.B., "*Law of Evidence relating to IT and forensic issues*" unpublished lecture notes
- Mahanamahewa, Dr. Prathiba *"Data Protection Law an E-Business and E-Government Perception" http://www.icter.org/ conference/sites/default/files/icter/IITC-2003p16.pdf accessed at 7.45am on 25 July 2016*
- http://money.usnews.com/money/personal-finance/articles/2016-01-07/10-banking-trends-for-2016
- ibid 62 above
- ibid 62 above
- ibid 62 above
- ibid 62 above
- ibid 62 above

- *"The 'SWIFT" Hack,'* The Sunday Times, Part Two, 31 July 2016 pg 14, (as reported by Krishna N Das and Jonathan Spicer)
- *"Lanka crucial error, but in Philippines the money disappeared,"* The Sunday Times, Part Two, 31 July 2016 pg 14, (as reported by Reuters)
- *https://www.law.cornell.edu/uscode/text/28/1651* accessed at 7.30am on 25 July 2016, *"All Writs Act"*
- http://www.time.com/427503/apple_fbi_iphone_case accessed at 7.15am on 04 June 2016
- ibid 71 above • ibid 70 above • ibid 71 above
- ibid 71 above
- Indatissa, Kalinga, *"Law Relating to Computer Crimes and a Commentary on the Computer Crimes Act No 24 of 2007"* (2008), pg. XI
- ibid 60 above
- *"Sri Lankan Attorney Elected to Cyber Crime Convention Bureau"* Sunday Times, dated 24 July 2016. Part 2, pg.18
- ibid 45 above