Article

E-COMMERCE ACT: STRAINING TO FIT IN

Ephyro Amatong
Theresa Ballelos
Rodolfo Ponferrada
Oliver Reyes

E-COMMERCE ACT: STRAINING TO FIT IN

Ephyro Amatong[*]
Theresa Ballelos[**]
Rodolfo Ponferrada[***]
Oliver Reyes[****]

I. INTRODUCTION

A popular truism within legal circles maintains that systems of law lag behind technology and practice. This is particularly true of commercial laws, such as the Law on Negotiable Instruments or the Law on Insurance, where the traditional paradigm has been that of usage and custom preceding codification into law. As a result, courts called upon to interpret commercial statutes have been able to look for guidance to the mercantile customs and usage which gave rise to them.

Put another way, the cart of the law has traditionally been drawn forward by the horse of technology and practice. The latter determines the direction of legal development, while the former is forever catching up – never to move ahead.

With the passage of the Electronic Commerce Act of 2000,[1] our legislature has discarded the traditional paradigm in favor of a new one, with the intention of spurring business forward. Yet unlike most of our commercial laws, the Act is not a codification of customs and usages past and present. It instead embodies provisions drawn from the Model Law developed by the United Nations Commission on International Trade Law (UNCITRAL), which in turn was drawn up from the smattering of experience derived by Western nations from their brief history of interaction with electronic commercial transactions. Especially as it can possibly apply within the Philippine context, it is intended to provide the engine for future economic development. It is anticipatory legislation.

---

[*] LL.B., UP College of Law (2001)
[**] LL.B., *cum laude* UP College of Law (2001), 6th place, 2001 Bar Examinations.
[***] LL.B., *cum laude* UP College of Law (2001), 1st place, 2001 Bar Examinations
[****] LL.B., UP College of Law (2001)

[1] Rep. Act No. 8792, signed into law by President Joseph E. Estrada on June 14, 2000. In an act drooping with symbolism, the president also affixed his digital signature to a presidential directive containing the implementing rules and regulations for E-Commerce Act.

This "forward-looking" characteristic of the law, while intended to facilitate the entry of the Philippines into the so-called "New Economy," also gives rise to serious problems of interpretation. Without existing Philippine practice to anchor it, many of the law's provisions are both highly technical and abstract. Nevertheless, as discussed below, its impact on our legal system is both direct and very real— with no shortage of enterprising individuals and businesses eager to make use of it.

With the E-Commerce Act, we have a law that is more advanced than our technology. The question now becomes, how is it to be applied and interpreted?

This paper will attempt to examine the effect of the E-Commerce Act on the Philippine legal system. We begin with a brief look at the present state of electronic commerce in the Philippines, together with some key concepts. We then proceed to examine the law itself – its objectives, its scope, and its key provisions – the recognition of electronic information as a functional equivalent of traditional writing. Next we provide a brief overview of the wide impact the Act has had on the body of Philippine law, the general problems that it may give rise to, and a general framework for responding to these problems. Finally, we examine in greater detail the effect of the Act on two key areas of Philippine Law – the Formation of Contracts and the Law of Evidence.

II. ELECTRONIC COMMERCE AND THE PHILIPPINES

A. What is E-Commerce?

The Act itself does not specifically define electronic commerce. During the period of interpellation of Senate Bill 1902[2], Senator Magsaysay, the bill's sponsor, defined "e-commerce" as a generic title which encompasses commercial and noncommercial electronic data transaction.[3] Alternative definitions include: "commercial transactions based on electronic transmission of data over communication networks such as the Internet;"[4] and "business conducted by using electronic communications and digital information processing technology."[5]

E-commerce can be traced to the introduction of electronic fund transfers between banks in the 1970s, later broadened by the electronic data interchange

---

[2] One of the Bills (together with House Bill 9971) which was merged to form the present Rep. Act No. 8792.

[3] Comm. on Trade and Commerce, S. Rpt. 179, 11th Cong., 66th Sess. (2000).

[4] E.C. Lallana, R. N. S. Quimbo and L. C. Salazar, *Business@ Philippines.com Electronic Commerce Policy Issues in the Philippines*, 3 POLICY DIGEST NO. 4 1, 2 (1999); quoting the Organization for Economic Cooperation and Development (OECD).

[5] *Ibid.* quoting APEC E-Commerce Task Force.

(EDI) and electronic mail (e-mail) in the 1980s. Further growth was encouraged by emergence of online services such as CompuServe and Genie, and drastically enhanced by the popularity of the Internet and the World Wide Web in the 1990s.[6]

E-commerce may either involve large-scale business to business (B2B) transactions such as those entered into by ShoeMart and its 500 suppliers;[7] or individual purchases made by consumers (B2C) over electronic networks similar to traditional catalog purchases.

The E-Commerce Act envisions B2B or B2C transactions through the medium of an Information and Communications System[8]—"Cyberspace" in popular speech. Using such an Information System, parties (denominated originator[9] and addressee[10]) communicate to each other via electronic data messages.[11] Communication through this medium is essentially anonymous—the originator and addressee need never see each other or even know each other.

Interest in e-commerce is spurred by the dramatic revenues reported by successful firms like online bookseller Amazon.com (US$ 1.2 billion in 1999); and the potential for equally dramatic reductions in cost. For instance, a face-to-face banking transaction with a teller in the United States was estimated at US 76 cents; an ATM transaction at US 43 cents; a telephone transaction at US 24 cents; and an Internet transaction at US 1 cent.[12]

---

[6] E.C. Lallana, R. N.S. Quimbo and L.C. Salazar, *Business@ Philippines.com Electronic Commerce Policy Issues in the Philippines*, 3 POLICY DIGEST NO. 4 1, 3 (1999) citing Ravi Kalakot and Andrew Whinston, ELECTRONIC COMMERCE: A MANAGER'S GUIDE 5 (1997).

[7] As cited by Senator Magsaysay in Committee Report 179, *supra* note 3.

[8] Rep. Act No. 8792 (2000), sec. 5 (d), "*'Information and Communication System'* refers to a system intended for and capable of generating, sending, receiving, storing or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or in which data is recorded or stored and any procedures related to the recording or storage of electronic data message or electronic document."

[9] Rep. Act No. 8792 (2000), sec. 5 (i),"*'Originator'* refers to a person by whom, or on whose behalf, the electronic document purports to have been created, generated and/or sent. The term does not include a person acting as an intermediary with respect to that electronic document."

[10] Rep. Act No. 8792 (2000), sec.5 (a) (2000), "*'Addressee'* refers to a person who is intended by the originator to receive the electronic data message or electronic document. The term does not include a person acting as an intermediary with respect to that electronic data message or electronic document."

[11] Rep. Act No. 8792 (2000), sec. 5 (c),*Electronic Data Message'* refers to information generated, sent, received or stored by electronic, optical or similar means."

[12] E.C. LALLANA, R.S. QUIMBO AND Z.B. ANDAM, E-PRIMER: AN INTRODUCTION TO E-COMMERCE 5 (2000). However, the initial optimism that characterized the so-called "internet economy" has subsequently been tempered by the burst of the Internet bubble.

B. E-Commerce in the Philippines

E-commerce as practiced in the Philippines faces dismal prospects. Investment group Jardine Fleming Exchange Capital categorically states that, despite the usual arguments for the Philippines becoming an Internet economy (e.g. numerous overseas Filipinos, English proficiency), "The Philippines is not a New Age economy."[13] In support of this view, Jardine Fleming points to the minimal amount spent by both individuals and businesses on e-commerce (a total of US$ 23.21 million in 1999—not even 2% of Amazon.com's total sales for the same year); low internet penetration (an estimated 320 thousand devices accessing the Internet in 1999); and the relatively high cost of internet access (the average monthly subscription cost in the Philippines is US$ 21.85, compared with US$ 4.74 in Malaysia and free access in Singapore).[14]

This is not to say that e-commerce is nonexistent in the Philippines. While there is no clear proof of tangible benefits, there are a number of significant Philippine companies which have embarked on some form of e-commerce. As earlier pointed out, retailer ShoeMart actively engages in B2B transactions. Furthermore, the three largest Philippine Banks (BPI, Metrobank and Equitable-PCI) and a host of other smaller banks now offer Internet banking. The Ayala Corporation, one of the country's largest conglomerates, has invested in both B2B and B2C services.

Local electronic commerce has also been bolstered on a surprising front—the cellular phone business. The phenomenal popularity of cellular phone usage and of short-messaging services has proved opportune for several local businesses to utilize the said technology for their own purposes. For now, most electronic transactions conducted through cellular systems are small in scale, and usually appurtenant to promotional campaigns.

Still most of these forays into e-commerce are fairly recent with the companies only now beginning to invest in the infrastructure needed for e-commerce.

---

[13] Jardine Fleming Research, PHILIPPINE INTERNET MANAGEMENT RULES 5 (2000).

[14] *Id.* at 6, 64-65 citing figures by International Data Corporation.

III. GENERAL OVERVIEW OF THE E-COMMERCE ACT

A. Objectives and Sphere of Application

It was with the avowed intent of improving and encouraging Philippine e-commerce that R.A. 8729 was enacted. As expressed in the E-Commerce Act, itself, its objectives are threefold:

> To facilitate domestic and international dealings...through the utilization of electronic, optical and similar medium, mode instrumentality and technology;
>
> To recognize the authenticity and reliability of electronic documents; and
>
> To promote the universal use of electronic transactions in the government and by the general public.[15]

To facilitate the achievement of these goals—in particular the universal use of electronic transactions—the E-Commerce Act mandates that all departments, bureaus, offices and agencies of the government, as well as all government-owned and-controlled corporations, transact their business and/or perform their functions using electronic data messages or electronic documents within two years from the effectivity of the Act.[16] The Act further mandates the installation of an electronic online network (RPWEB), within two years from its effectivity, to facilitate the open, speedy and efficient electronic online transmission, conveyance and use of electronic data messages or electronic documents amongst all government departments, agencies, bureaus, offices down to the division level.[17] The Department of Trade and Industry (DTI) is expressly designated as the lead agency for the direction and supervision of the promotion and development of electronic commerce in the country, with the power to promulgate rules and regulations, as well as provide quality standards or issue certifications.[18]

The E-Commerce Act intends to cover all electronic information, and is the governing law with respect to any kind of data message or electronic document used in the context of commercial and non-commercial activities. [19] Thus, unauthorized access or tampering with a private computer system[20] in a household, for instance, would still fall under the ambit of the E-Commerce Act.

---

[15] Rep. Act No. 8792 (2000), sec. 3.
[16] Rep. Act No. 8792 (2000), sec. 27.
[17] Rep. Act No. 8792 (2000), sec. 28.
[18] Rep. Act No. 8792 (2000), sec. 29.
[19] Rep. Act No. 8792 (2000), sec. 4.
[20] Penalized as hacking or cracking under Rep. Act No. 8792 (2000), sec.33 (a).

B. Legislative History of the E-Commerce Act

Considering that the E-Commerce Act is principally a domestic enactment of the UNCITRAL Model Law on E-Commerce,[21] the legislative histories of both enactments should be discussed.

In the national sphere, R.A. 8792 can be said to be the result of the harmonization of Senate Bill 1902 and House Bill 9971. Senate Bill 1902 was approved by the Senate on April 10, 2000 and thereafter transmitted to the House of Representatives.[22] The House then developed its own version of the Bill (H.B. 9971), which incorporated additional provisions (such as those on Transportation Documents) later adopted by the UNCITRAL. The two versions were consolidated by a Bicameral Conference Committee[23] prior to passage by both Houses of Congress and approval by the President on June 14, 2000.

A primary concern of both Houses was that the Act adhere as closely as possible to the UNCITRAL Model Law. During the period for interpellation of S.B. 1902, Senator Magsaysay emphasized that 80% of the Bill was based on the UNCITRAL Model Law.[24] During the proceedings of the Biacmeral Conference Committee tasked to harmonize the two versions of the act, the Chairpersons of both contingents emphasized adherence to the UNCITRAL Model as the basis of consolidation:

> THE CHAIRMAN (SEN. MAGSAYSAY): Briefly, the original version of the Senate and the original version of the House were very, very similar in the sense that it was the Senate version that we sent to the House to be filed. But along the way, of course, there are additions and some subtractions so we now have to put this together. My only frame of reference is that as long as the UNCITRAL Model law, substantially, is followed as closely as possible, we do not mind ...
>
> THE CHAIRMAN (REP. PUNZALAN). Well, we did it in the same way that the Senate did it, following the UNCITRAL Model. And the other provisions which have been included are basically the expansion only of the original versions or the original version that we had filed.[25] (emphasis supplied)

---

[21] G.A. Res. 51/162, U.N. GAOR, 29th Sess. (1996).

[22] Comm. Rpt. 179, *supra* note 3, 83rd Session (2000).

[23] Comm. on Trade and Commerce, Bicameral Conference Committee Report on the Disagreeing Provisions of S. No. 1902 and H. No. 9971, 11th Cong. (2000).

[24] Comm. Rpt. 179, *supra* note 3, 62nd Session (2000).

[25] Bicameral Conference Committee Report, *supra* note 23.

As implied from the above exchange and as readily seen from comparative readings of R.A 8792 and the UNCITRAL Model Law,[26] the bulk of the former is lifted almost word-for-word from the the latter.

C. Brief Legislative History of the UNCITRAL Model Law

In the international sphere, the legislative history of the UNCITRAL Model Law began when the U.N. Commission on International Trade Law considered a report of the Secretary-General entitled "Legal aspects of automatic data processing,"[27] at its seventeenth session in 1984, which identified several legal issues relating to the legal value of computer records, the requirement of a "writing", authentication, general conditions, liability and bills of lading. Since the legal problems identified were essentially those of international trade law, the UNCITRAL appeared to be the appropriate central forum to undertake and coordinate the necessary action.[28]

At its eighteenth session in 1985, the UNCITRAL considered a report on the "legal value of computer records"[29] which concluded that, on a global level, there were fewer problems in the use of data stored in computers as evidence in litigation than might have been expected. The more serious legal obstacle to the use of computers and computer-to-computer telecommunications in international trade appeared arise out of requirements that documents had to be signed or be in paper form.[30]

Eventually, the UNCITRAL came to the conclusion that it should undertake work towards establishing uniform legal rules on EDI. The goals of such work should be to facilitate the increased use of EDI and to meet the need for statutory provisions to be developed in the field of EDI, particularly with respect to such issues as formation of contracts; risk and liability of commercial partners and third-party service providers involved in EDI relationships; extended definitions of "writing" and "original" to be used in an EDI environment; and issues of negotiability and documents of title.[31] In 1992, the UNCITRAL, at its twenty-fifth session, and entrusted the preparation of legal rules on EDI to the Working Group

---

[26] Such as that appearing in Part II of THE ELECTRONIC COMMERCE ACT BUILDING THE NATIONAL ECONOMY ONLINE (Gilbert E. Lumantao, Margaret N. Uy, Ma. Cristina M. Atendido, eds., 2000).

[27] (A/CN.9/254)

[28] UNCITRAL Guide to Enactment of the Model Law, 29th Sess., Plenary (A/CN.9/426) (1996) par. 3.

[29] A/CN.9/265

[30] UNCITRAL Guide to Enactment of the Model Law, *supra* note 28 at par. 4.

[31] A/CN.9/360

on International Payments, which it renamed the Working Group on Electronic Data Interchange.[32]

After four years and the active participation of several member states, the Working Group completed the draft of the Model Law on Electronic Commerce which was adopted by the UNCITRAL during its 29th session in 1996, and subsequently favorably endorsed to member states by the UN General Assembly.[33]

The UNCITRAL continues to revise and update the Model Law. In 1998 it adopted the provision on Incorporation by Reference[34] proposed by the United Kingdom of Britain and Northern Ireland. It is now considering, among others, proposals to draft specific guidelines on digital signatures, possible liability of service providers and similar third parties, and new general rules to clarify how traditional contract functions (such as "performance" and "delivery") could be performed through electronic commerce.[35]

IV. THE HEART OF THE LAW – RECOGNITION OF ELECTRONIC DATA AND ELECTRONIC DOCUMENTS

A. Legal Recognition of Information Stored in Electronic Form

The E-Commerce Act explicitly recognizes the legal validity and enforceability of electronic data messages,[36] electronic documents,[37] and electronic signatures.[38] This legal recognition of information stored by electronic means is the heart of R.A. 8792.

In response to a query by Senator Serge Osmeña during the interpellation of S.B. 1902, Senator Magsaysay expressed the view:

> ...that the proposed e-commerce law was not trying to amend existing laws; it would simply establish a legal framework so that electronic document would be made admissible in court since the Civil Code only allows written documents to be admitted in court... the enactment of the bill into law would put the

---

[32] UNCITRAL Guide to Enactment of the Model Law, *supra* note 28 at pars. 6 – 15.

[33] UNCITRAL Model Law on E-Commerce, *supra* note 21.

[34] UNCITRAL Model Law on E-Commerce, *supra* note 21 at art. 5bis.

[35] *Report of the United Nations Commission on International Trade Law on the Work of its Twenty-ninth Session*, U.N. GEN. ASS OFF. REC. 55th Sess., Suppl. 17(A/51/17)(1996) at par. 218 to 211.

[36] Rep. Act No. 8792 (2000), secs. 5 (c), 6

[37] Rep. Act No. 8792 (2000), secs. 5 (f), 7

[38] Rep. Act No. 8792 (2000), secs. 8, 9

> Philippines at par with the rest of the world in the use of information technology, specifically e-commerce transactions.[39]

This view bears a striking resemblance with that of the UNCITRAL's:

> ...legal requirements prescribing the use of traditional paper-based documentation constitute the main obstacle to the development of modern means of communication. In the preparation of the Model Law, consideration was given to a possibility of dealing with impediments to the use of EDI posed by such requirements in national laws by way of an extension of the scope of such notions as "writing", "signature" and "original", with a view to encompassing computer-based techniques.[40]

Both the E-Commerce Act and the UNCITRAL Model Law are founded on the belief tnat legal recognition and enforceability of electronic information provide the key to increased e-commerce and enhanced world trade.

B. The Functional Equivalent Approach

The approach advocated by the UNCITRAL Model Law and adopted by the E-Commerce Act[41] is to view electronic information as the functional equivalent of traditional paper documents. Thus, virtual or non-physical paperless documents, such as those seen on a computer monitor screen, are deemed to perform the same function as physical paper documents.[42] It is based on an analysis of the purposes and functions of the traditional paper-based requirements with a view to determining how those purposes or functions could be fulfilled through Electronic Data Interchange (EDI) techniques.

> For example, among the functions served by a paper document are the following: to provide that a document would be legible by all; to provide that a document would remain unaltered over time; to allow for the reproduction of a document so that each party would hold a copy of the same data; to allow for the authentication of data by means of a signature; and to provide that a document would be in a form acceptable to public authorities and courts. It should be noted that in respect of all of the above-mentioned functions of paper, electronic records can provide the same level of security as paper and, in most cases, a much higher degree of reliability and speed, especially with respect to the identification of the source and content of the data, provided that a number of technical and legal requirements are met.[43]

---

[39] Comm. Rpt 179, *supra* note 3.
[40] UNCITRAL Guide to Enactment of the Model Law, *supra* note 28 at par. 30.
[41] Comm. Rpt. 179, sec. 7, last sentence of penultimate paragraph.
[42] Comm. Rpt. 179, *supra* note 3, 76th Sess. (2000).
[43] UNCITRAL Guide to Enactment of the Model Law, *supra* note 28 at par. 31.

Senator Magsaysay on the floor of the Senate expressed the exact same view.[44] UNCITRAL further clarified this functional equivalent approach by stating:

> The Model Law does not attempt to define a computer-based equivalent to any kind of paper document. Instead, it singles out basic functions of paper-based form requirements, with a view to providing criteria which, once they are met by data messages, enable such data messages to enjoy the same level of legal recognition as corresponding paper documents performing the same function.[45]

It should be noted that while the Model Law constantly refers to electronic information and e-mail, the principles on which the Model Law is based and its provisions were intended to apply also in the context of less advanced communication techniques, such as telecopy and facsimile. The Model Law makes allowances for situations where digitized information initially dispatched in the form of a standardized EDI message might, at some point in the communication chain between the sender and the recipient, be forwarded in the form of a computer-generated telex or in the form of a telecopy of a computer print-out.[46]

The documents that have proved most resistant to digital alternatives are those instruments conveying title to valuable personal property which have traditionally been notarized or required to be witnessed by two or more persons, such as real property deeds and wills. In such cases, a Notary Public is usually required to (at least in theory) screen the signers of such documents for identity, willingness, and basic awareness. However, optimists, confident of the entrepreneurial ingeniousness of the digital marketplace, believe that any technical or logistical challenge will not remain unsolved for long.[47]

C. Recognition of Electronic Documents

It is also curious to note that while the UNCITRAL Model Law refers only to "Electronic Data Messages" (EDM)[48] (perhaps to avoid complications that the term "document" might have given variations in the national laws of member countries), the E-Commerce Act further makes use of the term "Electronic Document" – the second word apparently used in its technical sense in the Philippine legal context.

---

[44] Comm. Rpt 179, *supra* note 42.

[45] UNCITRAL Guide to Enactment of the Model Law, *supra* note 28 at par. 33.

[46] UNCITRAL Guide to Enactment of the Model Law, *supra* note 28 at par. 26.

[47] C. N. Faerber, *Book Versus Byte: The Prospects and Desirability of a Paperless Society*, 17 THE JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW 797, 823-827 (1999).

[48] UNCITRAL Model Law on E-Commerce, *supra* note 28 at art. 2(a) "Data 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

Prior to the E-Commerce Act, a "document" was understood in two senses. First, under the Rules of Evidence, it was a deed, instrument or other duly authorized paper by which a fact is proved, affirmed or set forth.[49] Second, in substantive law, particularly Criminal Law, it is any written statement by which a right is established or an obligation extinguished.[50]

The Act explicitly recognizes electronic documents, by giving both evidentiary and substantive effect to "information or the representation of information... which is received, recorded, transmitted, stored, processed, retrieved or produced electronically;"[51] and places them on par with their traditional paper counterparts.[52]

As a result, the E-Commerce Act, rather than limiting itself strictly to economic transactions over electronic media, directly affects both the substantive and procedural/evidentiary aspects of Philippine law.

V. AREAS OF PHILIPPINE LAW AFFECTED BY THE COMMERCE ACT

A. Despite its specific purpose, the E-Commerce Act has had a broad impact on Philippine Law

This paper intends to discuss the impact of the E-Commerce Act on two key areas of Philippine Law—namely Contract Formation and the Law of Evidence. While a complete discussion of all the areas of Philippine Law affected by the E-Commerce Act are outside the scope of this paper, we feel it necessary to give at least a cursory enumeration of these areas to better illustrate the widespread change resulting from seemingly simple recognition of Electronic Data Messages and Electronic Documents.

---

[49] U.S. v. Orera, 11 Phil 597; People v. Camacho, 44 Phil 488

[50] People v. Moreno, 38 OG 120.

[51] Rep. Act No. 8792 (2000), sec. 5(f), "*'Electronic Document'* refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically."

[52] Rep. Act No. 8792 (2000), sec. 7, "Electronic documents shall have the legal effect, validity or enforceability as any other document or legal writing..."

1. Civil Law

a) Agency—Electronic Agents (Sec. 18(2)b)

Under the provisions of Section 18 of the Act, a purported Originator may be bound under an Electronic Data Message sent by: (1) an automatic pre-programmed information system, and (2) another person who had access to the Originator's method of authenticating Data Messages, even if the Originator repudiates or refuses to ratify the Data Message.[53]

The first case seems to introduce the idea of an electronic "agent" into Philippine law, whereby contract or instructions may be entered by a pre-programmed information system on behalf of the designated Originator. The second apparently introduces an exception to the law on agency wherein generally one cannot be bound by the unauthorized acts of another.

b) Preference of Credits – Effect on E-Banking Liabilities

The provisions of the law[54] provide that obligations incurred by a bank as a result of electronic transactions made through networking among banks, or linkages thereof with other entities or network are considered absolute and shall not be subject to the process of preference of credits under the Civil Code.

2. Criminal Law

For the first time, unauthorized access into or interference in a computer system (commonly called hacking or cracking) is penalized, apparently eliminating

---

[53] Rep. Act No. 8792 (2000), sec. 18, *Attribution of Electronic Data Message*

xxx

(2) As between the originator and the addressee, an electronic data message or electronic document 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 with respect to that electronic data message or electronic document; 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 an electronic data message or electronic document as being that of the originator, and to act on that assumption, if:

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

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

[54] Rep. Act No. 8792 (2000), sec. 16 ; DTI, DBM & BSP IMPLEMENTING RULES AND REGULATIONS OF THE E-COMMERCE ACT, Sec. 22 (2000).

the loophole which prevented criminal liability from attaching to the alleged author of the famous "Love Bug" virus.[55]

3. Commercial Law

a) Transportation – documentation affecting contracts of carriage of goods

The Act contains specific provisions concerning the validity of electronic contracts for the carriage of goods,[56] further modifying the Laws on Transportation

b) Intellectual Property

The Act specifies penalties for "pirating" intellectual property through telecommunications networks, apparently amending the applicable provisions of the Intellectual Property Code.[57]

Tax

While the avowed intent is for the E-Commerce Act to be tax neutral, there is considerable confusion (even among the legislators) as to the effect the Act on taxes such as the documentary stamp tax.[58]

---

[55] Rep. Act No. 8792 (2000), sec. 33 , *Penalties*. - The following Acts shall be penalized by fine and/or imprisonment, as follows:

(a) Hacking or cracking which refers to unauthorized access into or interference in a computer system/server or information and communication system; or any access in order to corrupt, alter, steal, or destroy using a computer or other similar information and communication devices, without the knowledge and consent of the owner of the computer or information and communications system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document shall be punished by a minimum fine of one hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years;

[56] Rep. Act No. 8792(2000), sec. 26.

[57] Rep. Act No. 8792 (2000), sec. 33, *Penalties*. - The following Acts shall be penalized by fine and/or imprisonment, as follows:

...

(b) Piracy or the unauthorized copying, reproduction, dissemination, distribution, importation, use, removal, alteration, substitution, modification, storage, uploading, downloading, communication, making available to the public, or broadcasting of protected material, electronic signature or copyrighted works including legally protected sound recordings or phonograms or information material on protected works, through the use of telecommunication networks, such as, but not limited to, the internet, in a manner that infringes intellectual property rights shall be punished by a minimum fine of one hundred thousand pesos (P100,000.00) and a maximum commensurate to the damage incurred and a mandatory imprisonment of six (6) months to three (3) years;

[58] Bicameral Conference Committee Report, *supra* at note 23.

Also, the statute provides that the rules on the place of dispatch and receipt of Electronic Data Messages or Electronic Documents also govern the tax situs of the transaction.[59] However, the practical application of these rules is unclear given that they establish the situs of transmission and receipt of Data Messages, and not the situs of a transaction or contract. Furthermore, this rule is subject to a qualification in the Implementing Rules that determination of tax situs by Sec. 23 shall only be to the extent not inconsistent with Philippine situs rules and the regulations which may be promulgated by the Bureau of Internal Revenue (BIR) relating to the tax treatment of electronic commerce transactions.[60]

On a more positive note, the Act provides that financial records required by law to be retained by a taxpayer—such as books of account for taxation purposes—may now be retained in a more compact electronic format.[61]

B. General Legal Problems Posed by the Implementation of the E-Commerce Act Within the Philippine Context

While the effects of the E-Commerce Act appear to be widespread, the provisions of the Act themselves are not anchored on familiar experience. The provisions of the law, for instance, on such as matters as authentication[62] and attribution[63] do not yield themselves to easy comprehension on first reading.

As already noted, the bulk of the E-Commerce Act has been a word-for-word adoption of the UNCITRAL Model Law. The rationale behind each provision was established, not during the Congressional Committee Hearing or during deliberations, but at the international level by the Working Group on Electronic Data Interchange. At the same time, the Model Law was intended as a "framework" law that does not itself set forth all the rules and regulations that may be necessary to implement all the techniques for recognition of electronic information in an enacting State. Accordingly, enacting States were expected to fill in the procedural details for procedures authorized by the Model Law and to take account of the specific, possibly changing, circumstances at play in the domestic sphere without compromising the objectives of the Model Law.[64]

---

[59] Rep. Act No. 8792 (2000), sec. 23.

[60] DTI, DBM & BSP IMPLEMENTING RULES AND REGULATIONS OF THE E-COMMERCE ACT, sec. 33 (2000).

[61] Rep. Act No. 8792 (2000), sec. 13 (a).

[62] Rep. Act No. 8792 (2000), sec. 11.

[63] Rep. Act No. 8792 (2000), sec. 18.

[64] UNCITRAL Guide to Enactment of the Model Law, *supra* note 28 par. 28.

While the Department of Trade and Industry has issued a set of Implementing Rules and Regulations, a side-by-side comparison with both R.A. 8792 and the UNCITRAL Model Law[65] show little in the way of substantial clarifications.

How then are we to apply an unfamiliar law, transplanted from an international legislature, which introduces revolutionary changes to both the substantive and procedural aspects of our Philippine legal system?

C. Approaches to Solving these Legal Problems

If confusion as to proper interpretation and application were the problem created by the unfamiliar and technical nature of the E-Commerce Act, the textbook response would be to make use of the tools of statutory construction in order to arrive at the spirit of the law. However, as we shall show later, such a response is not as straightforward as it might seem.

1. Legislative Intent

By and large the rationale for the provisions of the E-Commerce Act must be sought for in the Guide to the Enactment of the UNCITRAL Model Law. The Act itself provides for reference to the Model Law in case of need for guidance in statutory interpretation.[66]

Provisions which were added to the Model Law by our legislators include section 7 on the Legal Recognition of Electronic Documents; section 9 on Presumptions Relating to Electronic Signatures; section 11 on Authentication of Electronic Data Messages and Electronic Documents;[67] and section 19, Error on Electronic Message or Electronic Document.

2. Jurisprudential Interpretation

Prior to the enactment of R.A. 8792, there was scant Philippine jurisprudence touching on the admissibility of electronic information. The two leading cases which only passed on the matter tangentially are *People v. Burgos*[68] and

---

[65] Part II of Gilbert E. Lumantao, *supra* note 26.

[66] Rep. Act No. 8792 (2000), sec. 37 , *Statutory Interpretation.* - Unless otherwise expressly provided for, the interpretation of this Act shall give due regard to its international origin and the need to promote uniformity in its application and the observance of good faith in international trade relations. The generally accepted principles of international law and convention on electronic commerce shall likewise be considered.

[67] Introduced primarily by Senator Defensor Santiago in the basis of the Massachussetts draft of the Uniform Electronic Transactions Act dated December 23, 1999 as reported in Comm. Rpt. 179, *supra* note 3, 80th Sess. (2000).

[68] 200 SCRA 67 (1991).

IBM v. NLRC.[69] Both cases are touched on in our discussion of the effect of the Act on the Law of Evidence below.

It is not surprising that there is a dearth of Philippine jurisprudence on e-commerce problems. Resort will have to be made, at least initially, to persuasive cases from other countries such as the United States. Some of these cases are also discussed below.

3. Publicists

The writings of foreign publicists, as opposed to local sources, have proven more useful to date as a mode for interpreting general principles affecting electronic commerce. However, caution must be exercised when employing these authorities, as there are subtle differences even as between statutes enacted on the basis of the UNCITRAL Model Law.

4. Use of Presumption and Judicial Notice

Perhaps the most practical tool for an immediate application of the E-Commerce Act to real world problems are the presumptions created by the law itself, particularly as to Electronic Documents, Electronic Signatures, Attribution and Authentication. While these presumptions are highly technical in themselves (attribution being a good example), they nevertheless reduce the need for more technical proofs (such as that required to establish the tampering or hacking of a system).

The Supreme Court announced plans to amend the Rules of Court in order to take the changes created by the E-Commerce Act into consideration.[70] Perhaps these changes will contain more authoritative guidelines from the Court on how to evaluate and assess Electronic Data Messages and Electronic Documents offered as evidence.

We now proceed to discuss in greater detail two areas profoundly affected by R.A. 8927—the Law on Formation of Contracts and the Law of Evidence.

---

[69] G.R. No. 117221, April 13, 1999.

[70] *SC to amend rules to boost RP E-Commerce*, PHILIPPINE DAILY INQUIRER, March 12, 2001 at B18.

VI. CASE IN POINT: THE LAW OF CONTRACTS

A. Impact of the E-Commerce Act on the Formation of Contracts

1. Essential Elements of a Contract

For a valid contract to exist, the following requisites must be present: (1) Consent of the contracting parties, (2) Object certain which is the subject matter of the contract, and (3) Cause/Consideration for the contract.[71]

Of these essential requisites, the E-Commerce Act impacts on Consent—the meeting of the offer and the acceptance upon the thing and the cause which are to constitute the contract.[72] Consent must be manifested in some manner, and is now something that can be manifested electronically. Both the offer and the acceptance may be embodied in Electronic Data Messages.

2. Attribution

Because the parties to an exchange of Electronic Data Messages are essentially anonymous and may never see each other, a the law must set up framework whereby each party can trust and rely in good faith on the messages he or she receives from the other anonymous party. Originators must be bound by content of the Data Messages they send, and Addressees must be entitled to rely on the messages they receive as a basis for their actions. The E-Commerce Act establishes such a framework through a complicated set of presumptions.[73] The workings of this system are discussed in greater detail below.

3. Electronic Signatures as Consent and Authentication

A person's signature or inscription has historically been used for various purposes—as a means of signifying intent (to be bound, to signify approval, or some other intent), as a means of identifying the person signing, or as evidence of the integrity or genuineness of the document.[74] The E-Commerce Act explicitly

---

[71] CIVIL CODE, art. 1318.

[72] CIVIL CODE, art. 1319.

[73] Rep. Act No. 8792 (2000), sec. 28.

[74] T. J. Smedinghoff and R. H. Bro, *Moving with Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce*, 17 THE JOHN MARSHALL JOURNAL OF COMPUTER AND INFORMATION LAW 723, 731 (1991).

recognizes the electronic functional equivalents of traditional signatures[75] and gives to them the same legal effects[76]

B. Impact on the Form of Contracts

The general rule is that contracts are perfected by mere consent of the parties.[77] However, there are certain contracts which the law requires to be in a written form in order to be enforceable.[78]

Interestingly, the requisites for functional equivalence between an Electronic Document and a traditional paper document under the E-Commerce Act are stricter and more explicit than as found in the UNCITRAL Model Law. The UNCITRAL Model Law merely provides that "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."[79] While The E-Commerce Act explicitly provides that an Electronic Document is to be treated as the equivalent of a traditional written document provided: (1) it maintains its integrity, (2) it maintains its reliability, and (3) it can be authenticated so as to be usable for subsequent reference[80]

C. Problems Posed by the E-Commerce Act —Ensuring Attribution and Integrity

As adverted to earlier, a primary challenge to widespread acceptance of e-commerce as a means of doing business is the problem of the lack of trust in dealing with anonymous individuals.[81] In concrete terms, for an electronic document to serve as the functional equivalent of a traditional paper document, there must be a way of verifying: (1) if it has been properly attributed to the true Originator, and (2) if it has maintained its integrity.

---

[75] Rep. Act No. 8792 (2000), sec. 5 (e), "*'Electronic Signature'* refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document."

[76] Rep. Act No. 8792 (2000), sec. 9.

[77] CIVIL CODE, art. 1359.

[78] CIVIL CODE, art. 1403 (2).

[79] UNCITRAL Model Law, art. 6 (b),

[80] Rep. Act No. 8792 (2000), sec. 7 (a).

[81] E. C. Lallana, R. N. S. Quimbo and L. C. Salazar, *Business@ Philippines.com Electronic Commerce Policy Issues in the Philippines*, 3 POLICY DIGEST NO. 1, 5 (1999).

D. Proposed Solution: Public Key Infrastructure: The Solution to the Problems of Attribution and Integrity

Simply put, the problem of attribution means determining who sent the electronic message in an e-commerce transaction whereas the problem of integrity entails determining whether or not the message received is in an unaltered state. These problems are answered by what is known as Public Key Infrastructure. Public Key Infrastructure (PKI) or Public Key Cryptography or asymmetric public key system is a method for protecting the confidentiality, integrity, and authenticity of electronic messages such as those involved in electronic contracts.[82] It is a type of cryptography that is touted to be more suitable to the typical e-commerce transaction.[83] Michael J. Osty and Michael J. Pulcanio define a PKI as "a group of people providing necessary services to allow public key technology users to establish the authenticity of the public key of the people with whom they are transacting business."[84]

1. How does PKI work?

Public key cryptography involves the use of two codes (known as "keys") that are used by the signer of an electronic document to authenticate the source and content of his electronic documents, and by the recipient to validate their correctness.[85] In public key cryptography bboth th sender of the message and the recipient of the message are each given their own key pair, consisting of a secret "private key" and a publicly available "public key." The "private key" is kept solely in

---

[82] W. A. Effross, *Notes on PKI and Digital Negotiability: Would the Cybercourier Carry Luggage?* 38 JURIMETRICS J. 385 (1998). Effross highlights the advantages of PKI by illustrating the uncertainties inherent in other forms of security. He writes: "Public key cryptography as a method for protecting the confidentiality, integrity, and authenticity of messages has significant advantages over the more familiar forms of security involving such "symmetric single keys" as passwords or personal identification numbers. As one leading commentator has observed, in symmetric single key systems the sender (say, Alice) and the recipient (say, Bob) must trust each other not to reveal the password or "key, " which is used to both encrypt and decrypt the message, thereby weakening "non-repudiation"; that is, Alice may be able to deny that the message came from her by admitting that she had compromised the secrecy of the key by accusing Bob of having compromised it. Alice and Bob must also resort to a different key or an entirely different secure method in order to communicate this password initially to each other or to a third party (Connie) so that she can use their original key." PKI, which is also called the "asymmetric public key system," removes this problem by providing each participant with her own "key pair," consisting of a secret "private key" as well as a publicly available "public key."

[83] R. L. Mack, *Digital Signatures, The Electronic Economy and the Protection of National Security: Some Distinctions with an Economic Difference*, 17 THE JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW 981, 986 (1999).

[84] M. J. Osty & M. J. Pulcanio, *The Liability of Certification Authorities to Relying Third Parties*, 17 THE JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW 961 (1999).

[85] R. R. Jueneman and R. J. Robertson, Jr., *Biometrics and Digital Signatures in Electronic Commerce*, 38 JURIMETRICS J. 427, 438 (1998).

the possession of the signer of an electronic document and is used to encode the text of the document into the digital signature. The public key is made publicly available via some trustworthy publication procedure to any person, the "relying party" or the recipient of the message who may deal with the originator of the document.[86] To encrypt a message so that only the intended recipient could decipher it, the sender (or any other party) would obtain the recipient's public key and use a public-key algorithm, to send it to the recipient, who would decrypt it by applying his private key to the message. If another party, a third person who is not part of the transaction, received or intercepted this e-mail message it would be unintelligible to him because he could not, even knowing the recipient's public key, discover the recipient's private key.[87] That is because these keys, which are strings of alphanumeric characters, are mathematically linked to each other in such a way that they are complementary but at the same time, it is "computationally unfeasible to derive the secret key from the public key."[88] The relationship between the private and public keys is so complicated that it is "computationally infeasible" to deduce the private key solely from knowledge of the public key or to crate a signed message which can be verified by application of the public key without the knowledge of the private key. [89] To digitally sign an electronic document that an originator of the message ("sender") is sending to the recipient, the sender would apply his private key to the entire message or to a "digest" of it. When the recipient receives the message, he can decrypt it using the sender's public key; and since no one but the sender should have the sender's private key to digitally sign the message, the recipient can use the sender's public key to verify that the message came from the sender. Since the keys only allow the digital signature created by one of the keys to be decrypted or validated by the other key, a person receiving a digitally signed document that is verified by used of the public key knows that the document was signed by a person possessing the private key.[90] Moreover, because the signed form of the message incorporates not only information about the signer but also information about the

---

[86] *Ibid.*

[87] EFFROSS, *op. cit. supra* note 82 at 387.

[88] *Ibid.*

[89] JUENEMAN, *supra* note 85, "If many people need to verify the signer's digital signatures, the public key must be available or distributed to all of them, perhaps by publication in an on-line repository or directory where it is easily accessible. Although the keys of the pair are mathematically related, if the asymmetric cryptosystem has been designed and implemented securely it is "computationally infeasible" to derive the private key from knowledge of the public key. Thus, although many people may know the public key of a given signer and use it to verify that signer's signatures, they cannot discover that that (sic) signer's private key and use it to forge digital signatures. This is sometimes referred to as the principal of "irreversibility."

[90] *Ibid.* "The recipient verifies the digital signature by taking the text of the electronic document and converting it into a "hash result" using he same "hash function" as he originator and then applying the public key to the hash result. The process will result in verification if and only if th hash result of the original electronic document was encrypted by use of the private key to which the public key is related, to an extremely high level of confidence." A "hash result" is a shorter form of digital representation into which an electronic document is condensed in the creation of a digital signature.

content of the message itself, if the signed message has been tampered with en route to the recipient, his attempted verification of it using the sender's public key should fail.[91] This is because the signature uses the original text as an input to the encryption algorithm, if the message is altered in even the slightest way, the signature will not decrypt properly, showing that the message was altered in transit or that the signature was forged by copying it from a different message.[92] Thus, the digital signature process also assures the recipient of the integrity of the message.[93]

As illustrated above, PKI may be used to encrypt a message such that only the intended recipient would be able to decrypt the message and understand it. PKI may also be used to authenticate or digitally sign documents, by means of which the recipient may be able to verify that the message may be able to verify who the sender of the message is, and in the process of such verification, the recipient is also able to determine whether the integrity of the message was preserved. The combination of the two processes of message encryption and digital signing may be done in order to address the sender's concerns that his digitally signed message will be intercepted by someone other than the intended recipient.[94] The sender could encrypt for confidentiality his digitally signed message (the one prepared using his private key) with the public key of the recipient. Then, only the intended recipient would be in a position to decrypt it, and thus to read it and to verify to himself and to a third party that it had come to him unaltered form the sender.

2. The Certification Authority

As illustrated thus far, the only parties involved in an electronic commerce transaction within the PKI context are the sender (also known as the "subscriber" or "signer") and the recipient (also known as the "relying party"). It is to be noted however, that electronic commerce transactions are conducted between individuals who often has had no prior business relationship with each other.[95] In the use of PKI, these questions may arise: How can the sender be sure that in sending a message to the intended recipient he has the recipient's correct public key? Also, how can the recipient be sure that in decrypting the sender's message he has the

---

[91] EFFROSS, *op. cit. supra* note 82 at 387 – 388.

[92] *Id.* at 388 citing A. M. Froomkin, *Symposium: Innovation and the Information Environment: The Essential Role of Trusted Third Parties in Electronic Commerce*, 75 OR. L.REV. 49, 51 – 55 (1996).

[93] EFFROSS, *op. cit. supra.* note 82 at 388.

[94] *Ibid.* The adverse consequences of interception of a digitally signed message arises only if the digitally signed message is not encrypted for confidentiality by the sender. If the digitally signed message is not so encrypted, the unauthorized recipient can read it, verify to himself andto a third party that the sender signed it and also verify that it was not altered since the time it was signed by the sender. In order to protect against this possibility, the sender should encrypt the digitally signed message and thus ensure that only the intended recipient can decrypt it, read it, and verify to himself and to a third party that the message came to him from the sender in an unaltered state.

[95] OSTY, *op. cit. supra* note 84.

sender's correct public key instead of one of an impostor?"[96] In order to resolve these issues, public key systems have added "certification authorities" ("CAs").

3. Who is a certification authority (CA)?

A CA is an independent third party who ties a particular person to his public key.[97] CAs vouch for the proper match of party with public key and consequently with the unique private key that corresponds to the public key. CAs provide the parties with "certificates." These certificates, which are themselves digitally signed by the CA, corroborate one or more characteristics of the person to whom the certificate is issued—in this case, the party's identity and public key.[98]

The certification authority is responsible for deciding whether the digital signature is authentic. The certification authority provides a way by which the parties might more reliably identify a key pair to the entity with which they are communicating.

4. What exactly does the certification authority do?

The following description by Stephen Myers clearly details what the certification authority does:

> [D]uring an electronic transmission, the sender encodes a signature on the computer using the private key, and clicks on the sign document button By clicking on the sign document button, the digital signature is sent to a repository that stores the coded signature. The repository is the central storage area that warehouses electronic documents such a certification certificates of cybernotaries, lists of subscribers, and other information. The certification authority then contacts the computer's repository to see if the private key as sent corresponds to the public key of the intended recipient on file in the repository. If there is a match, the certification authority digitally signs the document and issues a computer-based certificate of authenticity, similar to the way that a notary would sign and seal a document to signify the validity of an original execution to a signature on paper.[99]

5. What does a CA's certificate contain?

A CA's certificate may typically contain "the identity of the issuing certification authority, identification of the subscriber, the subscriber's public key,

---

[96] EFFROSS, *op. cit. supra* note 82 at 388.

[97] OSTY, *op. cit. supra.* note 84 at 965.

[98] EFFROS, *op. cit. supra* note 82 at 388.

[99] S. G. Myers, *Potential Liability Under the Illinois Electronic Commerce Security Act: Is it a Risk Worth Taking?* 17 THE JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW 909, 919 – 920.

and the digital signature of the certification authority. It might also contain additional information, such as a certificate's expiration date, a statement of the certification authority's financial responsibility (or at least a reference to see the authority' repository for a detailed statement of financial responsibility), or the context in which the public key may be used."[100]

6. What is the process by which a CA creates and issues a certificate?

Several steps are involved in the process by which a CA creates and issues a certificate. Myers' identification of these steps is enlightening:

> First, the CA offering its certification services creates its own public and private key pair in the public key cryptography system. The CA's public key is widely available and recipients of messages trust the CA to have adequately protected its private key from becoming available to others.
>
> An applicant wishing to digitally sign a document creates a public and private key pair and then applies to the CA for a certificate. The certificate is the electronic record that will match the applicant to his public key and lists the public key as the "subject" of the certificate. The CA then takes the record containing the information to identify the applicant, who now is considered a 'subscriber,' the subscriber's public key, and the information identifying the CA, ad encrypts the record by signing it using its private key.
>
> The information collected and verified by the CA, as well as the CA's signature, serve as the completed certificate. The certificate is then made publicly available in a "repository" maintained by the CA or someone else. When the recipient receives the digitally signed message of the subscriber, which references the certificate, the recipient can choose to rely on the certificate and thereby become a "relying party." The recipient then goes to the repository, accesses the certificate that confirms the association of the signer to his public key, and retrieves a copy of the pubic key to decrypt the digital signature. Successfully decrypting the message with the public key is 'extraordinarily reliable evidence" that the message received was sent by the person holding the corresponding private key.[101]

7. Certification Authority v. Notary Public

The principal function of a certification authority is to bind the sender's private key with the recipient's public key, similar to the way that a notary public would sign and perhaps affix a seal to validate the original execution of a

---

[100] J. C. Anderson & M. L. Closen, *Document Authentication in Electronic Commerce: The Misleading Notary Public Analog for the Digital Signature Certification Authority*, 17 THE JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW 833, 853 (1999).

[101] MYERS, *op. cit. supra* note 99 at 965 – 66.

handwritten signature.[102] Thus, looking at the functions of a certification authority, one may be tempted to say that the certification authority is nothing more than a notary public working in cyberspace. There are indeed strong similarities between the two positions.[103] Among these similarities are the following:

a) Both are creatures of statute.
b) Both are typically licensed or commissioned by the state.
c) Both engage primarily in the process of identification.
d) Both occupy a position of public trust.
e) CAs will, as notaries now do, affect commercial transactions worth significant amounts of money annually.[104]

However, the differences between the certification authority and the traditional notary public far outweigh their commonalities.[105] **A certification authority is not the functional equivalent of a notary.** While CAs serve the same document signer identification function as notaries, CAs also verify the integrity of the substance of the documents to which the parties bind themselves. Furthermore, the potential magnitude and volume of transactions with which CAs will be called upon to deal distinguish the CA from the "relatively insignificant notary public." This additional function and unique work context justify the appellation that a CA is an "**enhanced or hybrid notary**".[106]

E. Electronic Signatures

1. Signature in a pen and ink world

The importance of a signature as a means of identification of the party being bound and of the intention of said party to be bound has long been recognized. "The written signature is regarded as the primary means of identifying the signer of a written document, based on the implicit assumption that a person's normal signature changes slowly and is very difficult to erase, alter, or forge without detection."[107]

---

[102] Jason Richards, *The Utah Digital Signature Act as "Model" Legislation: A Critical Analysis*, 17 THE JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW 873, 884 (1999).

[103] ANDERSON, *op. cit. supra* note 100 at 855. The similarities identified by Anderson and Closen are:

a)Both certification authorities and notaries public are created and regulated by statute.
b)Both possess the professional and legal duty to accurately identify document signers (without guaranteeing the proper identity of those signers).

[104] RICHARDS, *op. cit. supra* note 102 at 882.

[105] ANDERSON, *op. cit. supra* note 100 at 858 – 66.

[106] *Id.* at 868-869.

[107] JUENEMAN, *op. cit. supra* note 85 at 427.

A "signature" is defined as a "person's name, or a mark representing it, as signed or written by himself or by deputy, as in subscribing a letter or other document."[108] It is not a part of the substance of a transaction, but is instead a representation of that transaction.[109] To "sign" on the other hand, means "to engage by written agreement."[110]

2. Functions of the Signature: Moored in the Concept of its being a Manifestation of Consent

The value of a signature as the manifestation of a party's consent to a contract is brought to the fore when the functions of a signature are analyzed. The functions which a signature serves may be classified into evidentiary functions and ceremonial functions. The primary function of a signature is evidentiary, that is, a person's signature on a written document provides presumably reliable evidence of that person's assent to the terms contained in the writing.[111] Thus, while termed evidentiary, this function of the signature has its roots in the use of a signature as a manifestation of consent.

This evidentiary function relates to the twin purposes of a signature, which are "signer authentication" and "document authentication." Signer identification means identification that a distinctive form of signature is considered to be reliable evidence of the identity of the person signing the writing. By document authentication, on the other hand, a person's signature is also considered to be very reliable evidence that the signer assented to the terms contained in the written

---

[108] The RandomHouse College Dictionary (Rev. Ed.) 1223. Construction of the term "signature" within the legal framework of a paper-driven society has often been broad as to encompass any mark by which a person may be identified. A case in point is Arizona law, which illustrates the broad scope typically given to the word "signature" in a pen and ink world. Thus: "By Arizona statute, a signature is defined broadly and includes even a mark if the person cannot write. The Arizona version of the Uniform Commercial Code provides that a document can be signed with any symbol executed or adopted with a present intention to authenticate the writing. Early Arizona case law, which was based upon general common law, did not require any specific act for signing a legal document, regardless of the medium used to create signatures. One representative case states as follows:

> *The signature may be written by hand, or printed, or stamped, or typewritten, or engraved, or photographed, or cut from one instrument and attached to another. A signature lithographed on an instrument by a party is sufficient for the purpose of signing it, and it has been held that it is immaterial with what kin of an instrument a signature is made.*

The courts have even gone so far as to find that documents that were intended to be signed, but which were left unsigned through oversight, met applicable signature requirements. Similarly, a judge's unsigned search warrant was found valid because the failure to sign was an oversight. (B. P. Cotter and J. H. Messing, *Electronic Court Filing in the Pima County Small Claims Court --Technical Parameters, Adopted Solutions and Some of the Legal Issues Involved,* 38 JURIMETRICS J. 397, 404-405 (1998).

[109] MYERS, *op. cit. supra* note 99 at 915.

[110] The RandomHouse College Dictionary (Rev. Ed.)1223.

[111] JUENEMAN, *op. cit. supra* note 85 at 430.

document because of the assumed semi-permanent nature of ink on paper. The premise for this function is the difficulty of altering a written document without leaving detectable alteration marks.[112] Later, it will be seen that these twin purposes are the very same standards that govern signatures created in electronic media.

The ceremonial function of a signature, on the other hand, also has its moorings in the concept of signature as manifestation of consent. Also termed as the "psychological" or "cautionary" function, this function shows that the act of signing is one which calls to the signer's attention the fact that he is entering into a transaction that has legal consequences and may deter the signer from entering into hasty transactions.[113]

In addition to these two functions, Stephen Myers adds two more: one, that the signature is a sign of the signer's approval of the writing or the intent that the document be given legal effect, and two, that the signature is an "efficient tool" by bringing finality to the transaction and diminishing the subsequent need to inquire beyond the document's face.[114]

3. The E-Commerce Act and the Statute of Frauds

Only certain classes of contracts must be evidenced by a signed writing. The generic term "Statute of Frauds"[115] embodies the statutory requirement of a

---

[112] *Ibid.*

[113] *Id.* at 431.

[114] MYERS, *op. cit. supra* note 99 at 915 – 916.

[115] CIVIL CODE, art. 1403, par. 2 provides:

> Art.1403. The following contract are unenforceable, unless they are ratified:
>
> (2) Those that do not comply with the Statute of Frauds as set forth in this number. In the following cases an agreement hereafter made shall be unenforceable by action, unless the same, or some note or memorandum thereof, be in writing, and subscribed by the party charged, or by his agent; evidence, therefore, of the agreement cannot be received without the writing, or a secondary evidence of its contents:
>
> (a) An agreement that by its terms is not to be performed within a year from the making thereof;
> (b) A special promise to answer for the debt, default, or miscarriage of another;
> (c) An agreement made in consideration of marriage, other than a mutual promise to marry;
> (d) An agreement for the sale of goods, chattels or things in action, at a price not less than five hundred pesos, unless the buyer accept and receive part of such goods and chattels, or the evidences, or some of them, of such things in action, or pay at the time some part of the purchase money; but when a sale is made by auction and entry is made by the auctioneer in his sales book at the time of the sale, of the amount and kind of property sold, terms of

signed writing in order that a contract may be enforceable.[116] The question arises as to whether an electronic document qualifies as a "writing" that is "signed" as required by the Statute of Frauds. Most reform legislation in the United States specifically equates electronic documents with "signed writings' under the Statute of Frauds by equating virtually any electronic document with "writing." Some legislation, on the other hand, equate virtually any electronic mark or symbol with a signature."[117] Here in the Philippines, the Electronic Commerce Act of 2000 (R.A. 8792) does both. Sections 6 and 7 of the Act provide as follows:

> Sec. 6. *Legal Recognition of Data Messages.* - Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the data message purporting to give rise to such legal effect, or that it is merely referred to in that electronic data message.
>
> Sec. 7. *Legal Recognition of Electronic Documents.* – Electronic documents shall have the legal effect, validity or enforceability as any other document or legal writing, and -
>
> > (a) Where the law requires a document to be in writing, that requirement is met by an electronic document if the said electronic document maintains its integrity and reliability and can be authenticated so as to be usable for subsequent reference, in that -
>
> The electronic document has remained complete and unaltered, apart from the addition of any endorsement and any authorized change, or any change which arises in the normal course of communication, storage and display; and
>
> The electronic document is reliable in the light of the purpose for which it was generated and in the light of all the relevant circumstances.
>
> (b) Paragraph (a) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the document not being presented or retained in its original form.
>
> (c) Where the law requires that a document be presented or retained in its original form, that requirement is met by an electronic document if -
>
> There exists a reliable assurance as to the integrity of the document from the time when it was first generated in its final form; and
>
> That document is capable of being displayed to the person to whom it is to be presented: *Provided,* That no provision of this Act shall apply to vary any and all

---

sale, price, names of the purchasers and person on whose account the sale is made, it is a sufficient memorandum;

(e) An agreement for the leasing for a longer period than one year, or for the sale of real property or of an interest therein;

(f) A representation to the credit of a third person.

[116] JUENEMAN, *op. cit. supra* note 85 at 429.

[117] *Id.* at 434.

> requirements of existing laws on formalities required in the execution of documents for their validity.
>
> For evidentiary purposes, an electronic document shall be the functional equivalent of a written document under existing laws.
>
> This Act does not modify any statutory rule relating to the admissibility of electronic data messages or electronic documents, except the rules relating to authentication and best evidence.

Section 5 (e) of the Act defines electronic signature as follows: "Electronic Signature" refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document.

Moreover, Section 8 of the Act provides for the legal recognition of electronic signatures in this manner:

> Sec. 8. *Legal Recognition of Electronic Signatures.* - An electronic signature on the electronic document shall be equivalent to the signature of a person on a written document if that signature is proved by showing that a prescribed procedure, not alterable by the parties interested in the electronic document, existed under which -
>
> (a) A method is used to identify the party sought to be bound and to indicate said party's access to the electronic document necessary for his consent or approval through the electronic signature;
>
> (b) Said method is reliable and appropriate for the purpose for which the electronic document was generated or communicated, in the light of all the circumstances, including any relevant agreement;
>
> (c) It is necessary for the party sought to be bound, in order to proceed further with the transaction, to have executed or provided the electronic signature; and
>
> (d) The other party is authorized and enabled to verify the electronic signature and to make the decision to proceed with the transaction authenticated by the same.
>
> Sec. 9. *Presumption Relating to Electronic Signatures.* - In any proceedings involving an electronic signature, it shall be presumed that -
>
> (a) The electronic signature is the signature of the person to whom it correlates; and

> (b) The electronic signature was affixed by that person with the intention of signing or approving the electronic document unless the person relying on the electronically signed electronic document knows or has notice of defects in or unreliability of the signature or reliance on the electronic signature is not reasonable under the circumstances.

4. Attributes that an Electronic Signature Must Possess[118]

In the world of electronic commerce transactions and particularly within the PKI context discussed above, electronic signatures have assumed a great significance in authenticating both the originator of an electronic document as well as its content. With regard to the standards which are to govern signatures created through the electronic media, the theory has been advanced that an electronic signature should have two attributes:

> (1) signer authentication, which indicates who signed the document, and which should be difficult to produce by another without authorization; and
>
> (2) document authentication, which identifies the subject matter of the signing, making it impracticable to falsify or alter either the signed subject matter or the signature without detection.[119]

5. Defining the Digital Signature

a) The Unavoidable Contrast with the Handwritten Signature

Authorities are inconsistent in characterizing a digital signature vis-à-vis a handwritten signature. There are those who define a digital signature as the "functional equivalent or computer generated manifestation of a manual signature."[120] Others however, categorically declare that a digital signature is "not a computerized image of a handwritten signature."[121]

The conflict however, is more apparent than real. For while some authors equate a digital signature with a handwritten signature affixed in cyberspace, they are

---

[118] As stated earlier, it is interesting to note that the twin purposes of a signature in a pen and ink world are the very same attributes which an electronic signature must have.

[119] B. P. Cotter and J. H. Messing, *Electronic Court Filing in the Pima County Small Claims Court — Technical Parameters, Adopted Solutions and Some of the Legal Issues Involved*, 38 JURIMETRICS J. 397, 405 (1998) citing American Bar Association, DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND ELECTRONIC COMMERCE 6 –7 (1996).

[120] MYERS, *supra* at note 99 at 917 – 18 citing Michael L. Closen & R. Jason Richards, *Notaries Public-Lost In Cyberspace, or Key Business Professionals of the Future?*, 15 J. MARSHALL J. COMPUTER & INFO. L. 703, 735 (1997)

"A digital signature is the computerized version of a written signature." Osty, *supra* note 84 at 963.

[121] ANDERSON, *op. cit. supra* note 100 at 850.

quick to point out that it is not as simple as it sounds. A digital signature, unlike a handwritten signature, is created in several steps. It is made up of a series of digits representing a combination of the document and the unique computer-generated code, known as a "hash."[122] The highly technical process by which it is created and verified is described in detail by Michael J. Osty and Michael J. Pulcanio, thus:

> The signer first uses a "hash function" to encrypt the "message" that the signer is going to sign. The "hash function is a computer program used to create a unique hash result. These digits are a combination of letters, numbers, and/or symbols.
>
> Once the hash result is created, the message's signer types in a pseudo-PIN number, and then the private key generates a long string of numbers and letters which represents the signature. The computer-generated signature, like the hash result, is unique to each message.
>
> To verify the signature of a digitally signed message, the recipient reverses the process. Through the use of a software program on the recipient's computer, the message recipient computes a new hash result using the same has function that created the digital signature. With the public key of the signer and new hash result, the recipient then must determine tow components to verify the signature. First, whether the digital signature was created with the private key matching the public key; and second, whether the new hash result matched the original hash result created at the time the message was signed. A digital signature is "verified" if the public key successfully verifies the private key of the signer and the hash results match. This indicates that the document has not been altered between the sender and receiver.[123]

Thus, while a digital signature does serve as a means for identifying the sender of a message the way a traditional handwritten signature does, the process of creating a digital signature, the manner of verifying the same, and the additional functions it serves (i.e. apart from sender identification, it also serves as an indicator of integrity and an alteration deterrent) are so affected by the electronic media within which it is utilized that the digital signature may not be summarily dismissed as nothing more than a signature made in cyberspace.

b) Electronic Signature v. Digital Signature

It should be noted that there is a difference between "electronic signatures" and "digital signatures."

In the United States, there are two general categories of legislation related to electronic signatures: electronic signature legislation and digital signature legislation.

---

[122] OSTY, *op. cit. supra* note 84 at 963.
[123] *Id.* at 963-964.

These categories are technologically different from one another and yet they are often used interchangeably. The term "electronic signature" has been given numerous definitions. Illinois law defines it as "digital technology" whereas Florida law defines it as "any letters, characters, or symbols, manifested by electronic or similar means, executed or adopted by a party with an intent to authenticate a writing."[124] In the Philippines, the Electronic Commerce Act defines an *Electronic Signature* as "any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document."

The main difference between digital signatures and electronic signatures is that "the digital signature approach uses a specific type of technology, while the electronic signature method does not." To be more specific, "digital signature" is a term usually reserved for signatures which implement public key or asymmetric cryptographic systems, while "electronic signature" refers generically to any electronic technology intended by the party to validate writing. The distinction assumes legal significance when such signatures are involved in evidentiary proceedings. Digital signatures provide proof of message integrity and non-repudiation by the document signer. In contrast, electronic signatures are unverifiable and are vulnerable to forgery and repudiation by the signer.[125]

c) Implications of the Distinction between Electronic and Digital Signatures on the E-Commerce Act

It is worth noting that, despite the difference between electronic signatures and digital signatures, the e-commerce act does not provide for a definition of a "digital signature." Was this a deliberate omission because the digital signature is used largely within the context of a PKI and that since no PKI has been set up in the Philippines, a definition for "digital signature" would not be necessary? Another possible interpretation would be that the e-commerce act does not recognize that electronic signatures and digital signatures are distinct. Neither of these interpretations appears to be correct for a further analysis of the e-commerce act evinces recognition, implicitly at the very least, of the distinction between electronic signatures and digital signatures as well as the recognition of the existence of PKI.

First of all, the definition given in Section 5 (e) of the Act is consistent with the general, all-embracing scope of an electronic signature, that is, one that is not

---

[124] RICHARDS, *op. cit. supra* note 102 at 876 – 877.
[125] *Ibid.*

identified with any particular form of computer security in contrast to a digital signature which is largely deemed to be that used in a PKI context. Furthermore, and more significantly, in Sec. 5 (g) of the Act, a definition for "electronic key" is given as follows: g. *"Electronic Key"* refers to a secret code which secures and defends sensitive information that crosses over public channels into a form decipherable **only with a matching electronic key.** (emphasis supplied) The reference to a "matching electronic key" reveals a recognition of PKI since the matching key pairs is characteristic of the asymmetric public key system and is in fact, one of the hallmarks of PKI. It is also to be noted that Senator Tatad raised the question of whether or not the existence of a Public Key Infrastructure was a necessary condition for the enactment of the E-Commerce Act during the period for interpellation.[126] Be that as it may, in order to remove any ambiguity in the law and to preclude numerous and varying interpretations which may sow confusion in the implementation of the e-commerce act it is proposed that the e-commerce act include a definition of the term "digital signature."

6. In Praise of the Digital Signature: Its Advantages

Commentators sing praises for the digital signature. "A secure digital signature is believed to be the key to allowing technology to further revolutionize electronic commerce."[127] It accomplishes this goal in several ways:

> First, like a handwritten signature, a digital signature should **identify a document's signer**, and it should be **difficult to reproduce without permission**.
>
> Second, a digital signature verified by a certification authority **ensures the integrity of the document itself**, making it impossible or impracticable to alter it or its contents without detection.
>
> Third, a digital signature verified by a certification authority **eliminates the possibility of repudiation by the sender**.
>
> Finally, electronic documents can be encoded with a digital time stamp, **allowing transmission time to be ascertained.**[128](emphasis supplied)

---

[126] In response, however, Senator Magsaysay, the bill's sponsor, stated that he did not believe that PKI was necessary as the main entities involved are the two transacting parties, the originator and the addressee. It would have to depend on the parties whether they would need a certification authority and which entity would be acceptable to them. The bill does not provide for a certification authority to allow for flexibility. Senator Magsaysay cited the business practice of Shoemart where a third party is not needed as it accepts the integrity and reliability of its 500 suppliers. Committee Report No. 179, *supra* at note 3, 63rd Session (2000).

[127] ANDERSON, *op. cit. supra* note 100 at 849.

[128] *Id.* at 849-850.

The non-repudiation features of a secure digital signature assures the recipient that the sender cannot falsely deny that the document was sent, and it also prevents either party form unilaterally altering the terms of an agreement.[129]

F. PKI, Digital Signatures and Certification Authorities: The Benefits of A Compound Solution to a Complex Problem

PKI provides the environment within which digital signatures are utilized and certification authorities perform their functions. Within the context of the two key system (public key and private key) of the PKI, the digital signature is created with the use of private key, which in turn, is verified by the certification authority. The following are the benefits of this interrelated solution to the problems of attribution and integrity in electronic contracts.

> 1. It allows confidential communications between senders and recipients.[130] The encryption of electronic messages ensures that only the intended recipient is able to understand the message sent by the subscriber.

Since the private key is owned and kept by one person, PKI provides a degree of certainty that the confidential communication originated from the holder of the private key.[131] The mathematical link between the private and public keys as well the principle of irreversibility at work allows the recipient to identify with nearly mathematical certainty the sender of the message. The identity of the party giving (or withholding) his consent to a contract is thereby clearly established.

> 2. The digital signatures verified by a certification authority assures the recipient that the sender cannot falsely deny that the document was sent. The matching of the key pairs in the PKI thereby precludes the possibility of repudiation by the sender.

With the use of digital signatures, the parties to an electronic contract are likewise assured of the integrity of the electronic message. Through the verification process employed on the digital signature and the technical workings of the hash result,[132] the recipient is assured that he received the message in an unaltered state. Moreover, since the digital signature and he hash result is unique to each message, the parties are prevented from unilaterally altering the terms of an agreement without it being detected.

---

[129] *Id.* at 850.

[130] MACK, *op. cit. supra* note 83 at 986.

[131] *Ibid.*

[132] "[A]ny alterations to a message produces a new hash result when the same hash function is used." OSTY, *op. cit. supra* note 84 at 249.

> 3. With the participation of certification authorities, heightened security is given to the e-commerce transaction in that the recipient is assured that the sender is indeed who he or she purports to be. Certification authorities add another level of authentication to the e-commerce transaction when they issue digital certificates which confirm the identities of individuals and the ownership status of key pairs. Through them, a further verification of the sender's identity is achieved.[133]

Some claim that digital signatures verified by certification authorities within the PKI context are impregnable. But, others caution that "no security scheme is 100% unbreakable."[134]

Human involvement is a present in every system. A concomitant result of that involvement is the ever-present prospect of human error. In the system of digital signatures verified by certification authorities, there are also areas vulnerable to human follies. For one, the private key can assure communication only if it is kept truly private by the people who control it. Devious characters can dupe unsuspecting private key holders into divulging their codes to these impostors. Moreover, the confidentiality of the contents of electronic communications may be placed in jeopardy simply because of the all too human element acting in senders of messages and holders of information who simply do not take sufficient security steps to prevent unwanted disclosures. As observed by Anderson and Closen, "[t]here s no reason to expect that the people who serve as certification authorities will rise above the same kinds of misconduct that have been committed by private individuals and public officers at every level."[135] It is thus imperative that rigorous process of giving out of credentials[136] of CAs as well as the prescribing of a Code of Ethics and Professional Responsibility[137] for certification authorities be enacted to counteract these possible problems.

The need for the interrelated solution of PKI, digital signatures and certification authorities is undeniable.[138] As stated above, subject of course to the

---

[133] MACK, *op. cit. supra* note 83 at 987.

[134] ANDERSON, *op. cit. supra* note 100 at 869.

[135] *Id.* at 870.

[136] *Ibid.*

[137] D. Athanasopoulos-Arvanitakis & M. J. Dye, *A Proposed Code of Professional Responsibility for Certification Authorities*, 17 THE JOHN MARSHALL JOURNAL OF COMPUTER & INFORMATION LAW 1003 (1999).

[138] MACK, *op. cit. supra* note 83 at 981. "The expansion of e-commerce transactions and the tremendous opportunities and benefits available to merchants and consumers will not be realized unless there are mechanisms to ensure that online transactions are authentic and verifiable. Digital signatures clearly provide that mechanism. *Id.* at 1001.

limitations thus presented, the benefits provided by this integrated solution would help achieve the goals of the e-commerce act.[139]

It is hereby proposed that Public Key Infrastructure be established in the country in order that the problems of attribution and integrity may be addressed. In line with this, it is also proposed that the e-commerce act be amended so as to include the definitions of "Public Key Infrastructure" as well as a definition of "digital signature"[140] in order to remove ambiguities in the law and provide explicit legal recognition of these two concepts. In addition, it is proposed that certification authorities, given the vital function they play in e-commerce transaction, also be recognized in the e-commerce act or in a separate law. It is furthermore proposed that qualifications for certification authorities, enumeration of functions, guidelines as to performance and a code of ethics for certification authorities be included in the e-commerce act or enacted as a separate law.

VII. CASE IN POINT: THE LAW OF EVIDENCE

A. Notification/Service and Filing via Electronic Data

Heretofore, the only permissible modes of serving and filing pleadings, judgments and other papers under Philippine rules of procedure are either in person or by mail. Specifically, the rules of procedure provide that the manner of filing shall be as follows:

> The filing of pleadings, appearances, motions, notices, orders, judgments and all other papers shall be made by presenting the original copies thereof, plainly indicated as such, personally to the clerk of court or by sending them by registered mail.[141]

---

[139] It is interesting to note how our legislators addressed the questions of PKI and certification authority necessity during the Senate deliberations. The question of whether or not the existence of a Public Key Infrastructure was a necessary condition for the enactment of the E-Commerce Act was raised during the period for interpellation by Senator Tatad. In response, Senator Magsaysay, the bills sponsor, stated that he did not believe that PKI was necessary as the main entities involved are the two transacting parties, the originator and the addressee. It would have to depend on the parties whether they would need a certification authority and which entity would be acceptable to them. Moreover, the bill does not provide for a certification authority to allow for flexibility. Senator Magsaysay cited the business practice of Shoemart where a third party is not needed as it accepts the integrity and reliability of its 500 suppliers. Comm. Rpt. 179, *supra.* at note 3, 63rd Session (2000).

[140] "The government should take the lead in promoting entry into the global Internet economy by establishing minimal uniform standards that provide legal recognition for digital signatures. MACK, *op. cit. supra* note 83 at 1001.

[141] RULES OF COURT, Rule 13, sec. 3.

Regarding the modes of service, the rules provide that "[s]ervice of pleadings, notices, orders, judgments and other papers shall be made either personally or by mail."[142] And finally, for judgments, final orders or resolutions, the rules likewise require that they be served either personally or by registered mail.[143]

Did the advent of the E-Commerce Act add another mode of service and filing? The E-Commerce Act is not clear on this matter. However, a collective reading of various provisions of the law and its implementing rules would provide a very plausible, if not strong, argument that indeed, the E-Commerce Act has added or intends to add another mode of service and filing.

In part, the law provides that:

> Notwithstanding any law to the contrary, within two (2) years from the date of the effectivity of this Act, all departments, bureaus, offices and agencies of the government, as well as all government-owned and-controlled corporations, that pursuant to law require or accept the filing of documents, require that documents be created, or retained and/or submitted, issue permits, licenses or certificates of registration or approval, or provide for the method and manner of payment or settlement of fees and other obligations to the government, shall -
>
> (a) accept the creation, filing or retention of such documents in the form of electronic data messages or electronic documents;
>
> (b) issue permits, licenses, or approval in the form of electronic data messages or electronic documents;
>
> (c) require and/or accept payments, and issue receipts acknowledging such payments, through systems using electronic data messages or electronic documents; or transact the government business and/or perform governmental functions using electronic data messages or electronic documents, and for the purpose, are authorized to adopt and promulgate, after appropriate public hearing and with due publication in newspapers of general circulation, the appropriate rules, regulations, or guidelines, to, among others, specify –
>
> - the manner and format in which such electronic data messages or electronic documents shall be filed, created, retained or issued;
>
> - where and when such electronic data messages or electronic documents have to be signed, the use of a electronic signature, the type of electronic signature required;

---

[142] RULES OF COURT, Rule 13, sec. 5.

[143] RULES OF COURT, Rule 13, sec. 9. This section also provides that in case of a party summoned by publication who has failed to appear in the action; judgments, final orders or resolutions against him shall be served upon him, in addition to service by mail, also by publication at the expense of the prevailing party.

> - the format of an electronic data message or electronic document and the manner the electronic signature shall be affixed to the electronic data message or electronic document;
>
> - the control processes and procedures as appropriate to ensure adequate integrity, security and confidentiality of electronic data messages or electronic documents or records or payments;
>
> - other attributes required of electronic data messages or electronic documents or payments; and
>
> - the full or limited use of the documents and papers for compliance with the government requirements: Provided, That this Act shall by itself mandate any department of the government, organ of state or statutory corporation to accept or issue any document in the form of electronic data messages or electronic documents upon the adoption, promulgation and publication of the appropriate rules, regulations, or guidelines.[144]

A cursory reading of the above-quoted provision would lead one to conclude that the said provision does not apply to the judiciary but only to the executive department; the term "department" as used in the quoted provision referring to the various executive departments (e.g., Department of Tourism, Department of Trade and Industry, etc.) rather than to the judiciary, legislature and the executive as the three equal and coordinate departments of the Republic. However, taking into consideration the corresponding implementing rule, one would be made to think again. The said corresponding implementing rule, after stating *in toto* the provision of law, further provides that:

> Nothing in the Act or the Rules authorizes any person to require any branch, department, agency, bureau, or instrumentality of government to accept or process electronic data messages; conduct its business; or perform its functions by electronic means, until the adoption, promulgation and publication of the afore-mentioned appropriate rules, regulations or guidelines. Such rules, regulations or guidelines as well as the underlying technologies utilized in the implementation of the Act and these Rules shall conform the principles set forth in the immediately succeeding section. [145]

It is submitted that the inclusion of the word "branch" signifies nothing else but the intention of the law, as interpreted by the government agencies empowered by law to enforce the provisions of the act and issue the necessary implementing rules and regulations,[146] for its provisions to apply to all the three

---

[144] Rep. Act No. 8792 (2000), sec. 27.

[145] DTI, DBM & BSP IMPLEMENTING RULES AND REGULATIONS OF THE ELECTRONIC COMMERCE ACT, sec. 37, last paragraph (2000).

[146] Rep. Act No. 8792 (2000), sec. 34.

branches of government. Taken in consonance with one of the over-all objectives of the E-Commerce Act, that is, "to promote the universal use of electronic transaction in the government and general public,"[147] conclude that the Act intended to give validity to the electronic filing of pleadings, judgments and other court-related documents, subject of course to the adoption of the appropriate rules, regulations and guidelines.

Reading the rule that provides that "a requirement under law for a person to provide information in writing to another person is satisfied by the provision of the information in an electronic data message or electronic document [emphasis supplied]"[148] in the same light would also lead one to conclude that the law intended to give efficacy to electronic service of court-related documents. Service of court-related documents is to information to another person, in particular the other party or parties in a case, that the court-related documents being served will be filed with the court.

Allowing the electronic filing or submission of documents is but a logical consequence of deeming electronic contracts as a generic class, binding. The issues attendant to the authentication as to the source of these pleadings or papers are similarly situated to those issues pertaining to the authentication of electronic contracts. Other aspects of electronic filing could also find their equivalent circumstances attaching to the electronic contracts. These two systems are subsumed under one paradigm; hence, the resolution of whatever legal problems that may arise out of one subset should necessarily affect the other subset. This point should be considered by the delegated rule-makers, such as the Philippine Supreme Court tasked with enacting rules of procedure.[149]

B. Electronic Data as Evidence

The E-Commerce Act is very explicit insofar as its impact on the evidentiary rules relating to authentication and best evidence. While it ostensibly does not modify any statutory rule relating to the admissibility of electronic data messages or electronic documents; it provides as exceptions the rules on authentication and best evidence.[150] While it is clear that the law modified the rules on authentication and best evidence, it is not so clear as far as the parol evidence rule is concerned.

---

[147] Rep. Act No. 8792 (2000), sec. 3.

[148] DTI, DBM & BSP IMPLEMENTING RULES AND REGULATIONS OF THE ELECTRONIC COMMERCE ACT, sec. 7(b) (2000).

[149] CONST., art. VIII, sec. 5, par. (5); RULES OF COURT, Rule 1, sec. 2.

[150] Rep. Act No. 8792 (2000), sec. 7, last paragraph.

Taking the same provision alone and at face value, one can easily conclude that the parol evidence rule has not been nor was intended to be modified. But considering certain provisions of the E-Commerce Act and its implementing rules, it may be argued the rule on parol evidence was modified.

The primary reason for holding that the parol evidence rule may have been modified is the rule on incorporation by reference. The law provides that "[i]nformation shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the data message purporting to give rise to such legal effect, or that it is **merely referred to** in that electronic data message." [151] *(emphasis supplied)* The corresponding implementing rule is more direct as it provides that "[i]nformation shall not be denied validity or enforceability solely on the ground that it is not contained in an electronic data message or electronic documents but is merely **incorporated by reference** therein."[152] *(emphasis supplied)*

The rationale behind the parol evidence rule is the understanding that "when the parties have reduced their agreement on a particular matter into writing, all their previous and contemporaneous agreements on the matter are merged therein, hence evidence of a prior or contemporaneous verbal agreement is generally not admissible to vary, contradict, or defeat the operation of a valid instrument."[153] The rules presume that having gone through all the trouble of reducing their agreement into writing, the parties have ensured that all the matters they have agreed upon are contained in the said agreement.

When it comes to incorporating another document by reference, the usual practice has been to mention in the incorporating document that the incorporated document is "incorporated by reference as fully set forth herein" and the "incorporated document is attached or accompanies the incorporating document."[154]

Because the incorporated document is physically attached to the main incorporating document, there is almost no problem that the parties are put on notice that there was a document incorporated by reference in their main agreement.

However, with the advent of electronic documents, a big possibility that a notification problem may arise if documents, likewise electronic, are incorporated by reference in the main electronic document. A question inevitable arises as to why one cannot simply make a long electronic document setting forth all relevant

---

[151] Rep. Act No. 8792 (2000), sec. 6.

[152] DTI, DBM & BSP IMPLEMENTING RULES AND REGULATIONS OF THE ELECTRONIC COMMERCE ACT, sec. 8 (2000).

[153] 2 FLORENZ D. REGALADO, REMEDIAL LAW COMPENDIUM 451-452 (1989).

[154] S. S. Wu, *Incorporation by Reference and Public Key Infrastructures: Moving the Law Beyond the Paper-Based World*, 38 JURIMETRICS J. 317, 318-319 (1988).

provisions so that incorporation by reference may be done away with. As keenly observed by one writer:

> Businesses have a great incentive, from a marketing and sales perspective to make web-based contracts as short as possible. Short contracts may improve the user's experience on the web sites. Longer contracts can be perceived as bogging the user down in legalese, making users impatient, and possibly dampening sales. Legal counsel for such companies, though, may urge them to have complete contracts containing all the terms deemed essential to this type of agreement. The change in the medium from paper to electronic form has not changed these businesses' need for protective clauses in such agreements. How then can these businesses resolve the tension between the legal need for comprehensive contracts and the marketing and sales desire for short contracts?[155]

The obvious answer to his question is "incorporation by reference." Taking into consideration the peculiar nature of electronic documents, it has been the current practice to incorporate electronic documents by hypertext linking. One author describes hypertext linking in this manner:

> A more subtle form of incorporation by reference, however, occurs when a company simply places a few words on a web page and ties the words to a document containing contractual terms by using a hypertext link. Web sites use words or phrases such as 'Disclaimer', 'Important Legal Information', and 'Important Disclaimers and Legal Information' to call attention to a hypertext-linked document setting forth terms and conditions. This words and phrases though, do not themselves indicate an incorporation. Rather, the nature of the hypertext link itself acts as a reference to the disclaimers and legal information.[156]

Considering that in cases of incorporation by reference it is crucial that the incorporation be brought to the attention of the adhering or consumer party for purposes of satisfying the need for informed consent,[157] incorporation by reference using hypertext linking poses a big problem. Usually, consumers disregard or don't pay attention to ostensibly innocuous hypertexts linked to the main document.

---

[155] *Id.* at 324-325.

[156] *Id.* at 320.

[157] V. Wattiez Larose, *Brief Essay on the Notion of and Rules Relating to Incorporation by Reference in Civil Law Systems*, 38 JURIMETRICS J. 295, 297 (1998).

C. Problems Posed by the E-Commerce Act and Proposed Solutions

1. Notification/Service and Filing via Electronic Data

In trying to solve the technology design problem, one can learn a thing or two from the experience of Pima County court officials.[158] Court officials of Pima County, Arizona, U.S.A. initiated the daunting task of offering electronic filing of pleadings and other documents over the Internet for small claims court.

A problem arose as to what technical solution to adopt. Given the nature of the small claims court, that is, informal and popular, the court officials were unwilling to adopt any technical solution that compromised trouble-free access to the court by the general public. Thus, the court officials discarded the use of plug-ins, even free ones, that enable uniform document formatting and printing over many Internet computer platforms, because of the potential difficulties users might encounter in installing the plug-ins, or in achieving trouble-free results during operation.

Likewise rejected for being impractical was pre-registration of electronic filers with the small claims court in advance of electronic filing, for the purpose of issuing digital identifiers such as passwords or digital certificates. Although pre-registration and the corresponding use of digital identifiers may weed out impostors and other nuisance and abusive filers, the additional inconvenience was considered unacceptable for impeding on the unrestricted use of the court system. For the same practical considerations, the compulsory use of digital and/or electronic signatures was rejected.

What technological design then did the county court officials choose? They chose a simple design where electronic filers are initially authenticated through a combination of unique personal information and the credit card account used to pay for the filing, provided by the filing party at the time of filing. Examples of unique personal information would be the maiden name of the filer's mother, his social security number or driver's license number. Based on this combined information, the filers are then given access to forms that collect information that is used to process and assemble the complaints and answers used in small claims cases.

The combined information signed and submitted by electronic filers is then memorialized by a digitally signed receipt from the court, which is immediately generated and returned to the e-mail address that was supplied by the filing party

---

[158] COTTER, *op. cit. supra* note 119.

during the information collection stage of the filing furnishing the court's e-mail address with a copy. The said digitally signed receipt is the authentic record of filing and not any paper copy of the pleading electronically filed. This system allows for self-checking in this wise: if the electronic filer does not have access to the e-mail address furnished at the time of filing, the filer will only have difficulty, if at all, producing the authentic digital record of the filing. Notification that a receipt was unable to be delivered will alert the court officials to a mishap in transmission, which may be caused by an attempted fraudulent filing. On the other hand, if the e-mail address where the information was sent actually belongs to the filer, this fact can be of limited assistance in confirming the probable true identity of the filing party, assuming that unauthorized, undetected access to the filer's mail box by an intruder did not take place.

This simple authentication process provides a "sufficient base-line" for the presumption that "a pleading which was digitally signed by the court is authentic, unless a party can establish to the satisfaction of a judge that the party did not originate the pleading" to arise.[159] Against the charge that such is very susceptible to fraud, court officials argue that the said system is consistent with the current custom and practice as far as paper document filing is concerned considering that "no identity check is performed with respect to original pen and ink signatures on paper documents today." Pen and ink signatures are presumed valid, unless a party proves otherwise.[160]

Naturally, one would argue that such a system worked for Pima County because it only involves cases in small claims courts. But nonetheless, there are important lessons that can be gleaned from the county's experience.

First, a very elaborate technical solution is not necessary. The most common reason forwarded for choosing the most complicated technology available is to prevent fraud and forgery. But the general experience of human kind shows that no amount of sophistication can match the wit and skill of a determined forger. It is consolation enough that such forgers and fraud artisans do not predominate, and that most are found out and caught in time.

Moreover, an overly technical solution is hard to understand and therefore, breeds non-compliance. A simple technical solution that is understood by the general public would suffice as long as it is technologically adequate enough to provide the basis for the second lesson to be learned: presume both the filing and the filed document to be valid provide the said basis is laid, unless proven otherwise.

---

[159] *Id.* at 403.
[160] *Ibid.*

2. Presentation in Judicial Proceedings

With the advent of electronic documents and electronic data messages, a practical problem arises. How does one present an electronic document or electronic data message as evidence in a judicial proceeding? What exactly would be presented? Would it be the hard disk or the floppy disk that contains the electronic data? Would a computer printout suffice? Does one need to present the encoder? Who exactly does one have to present to authenticate the electronic evidence?

Moreover, what type of evidence would the electronic document or data message consist of? Would electronic evidence be considered real or object evidence? If so, what exactly would be addressed to the senses of the court? The floppy disk? The hard disk? The monitor? Some other computer or electronic paraphernalia? Testimony from an expert necessary to interpret the real evidence for the court? Or maybe just the testimony of the one who encoded the document or of anyone who had anything to do with its production? If the evidence were considered documentary, what type of printout would suffice? What kind of printout would successfully defeat any objection on the ground of best evidence?

Fortunately or unfortunately, Philippine practice has not been beset by these problems so pervasively that Philippine jurisprudence has not been given enough chances to develop rules regarding electronic evidence. To date, there have been only two cases that have reached the Supreme Court that have at least tangentially touched on electronic evidence. The first is a sedition case involving diskettes. While the second one is a labor case involving e-mails.
In the first case[161], the prosecution offered in evidence certain diskettes seized from the accused. The accused objected to the offer arguing that they have been tampered. The lower court sustained the accused and disallowed the admission of the diskettes, specifically the act printing out the contents of the said diskettes. On review, the Supreme Court ruled that the diskettes were admissible on the basis of the regularity in the performance of public service considering that there was showing that the diskettes could have been tampered with. To allay the fears of the judge, the court suggested that the printing out of the contents be conducted by an entity acceptable to all parties, especially the judge.

In the second case,[162] the employer sought to present printouts of e-mails to prove that the dismissal of the employee was attended with due process. The labor arbiter admitted the printouts. The National Labor Relations Commission (NLRC) disagreed. On review, the Supreme Court agreed with the NLRC, ruling that the printouts could not be admitted because it was not signed by anybody, either the

[161] People v. Burgos, G.R. No. 92739. August 2, 1991, 200 SCRA 67.
[162] IBM Philippines, Inc. v. NLRC, G.R. No. 117221, April 13, 1999, 305 SCRA 592.

sender or receiver and there was no proof regarding the reliability and integrity that the computer system that produced the said printouts.

The Philippine rules of procedure classify pieces of evidence into three. There is object or real evidence that refer to "those addressed to the senses of the court."[163] Then there is documentary evidence which consists of "writings or any material containing letters, words, numbers, figures, symbols or other modes of written expressions offered as proof of their contents."[164] And finally, there is testimonial evidence which is the "assertions made on the witness stand nod any assertion taken as the basis of an inference to the existence of the matter asserted whether made in court or not."[165]

Under the E-Commerce Act, the problem of classification is at least solved. Electronic evidence is in the nature of documentary evidence. Electronic documents are functional equivalents of written documents.[166] If the E-Commerce law had any indispensable provision, it is that which essentially says that electronic documents should be treated the same as traditional written documents.

However, as adverted to earlier, a problem arises as to what particular manifestation of the electronic document has to be presented? Would the so-called soft copy suffice? Or is the paper-printed hard copy needed? Or maybe yet, the document as it appears from an output monitor?

It is submitted that, if full efficacy were to be given the law, any manifestation would do. Nevertheless, to solve practical problems, a computer printout on paper is best advised to be the one presented in court. If time comes when the courts of law are technologically equipped to receive in evidence soft copies and or view electronic evidence from monitors, then the litigant would have a choice. Considering the rapid pace at which the computer industry has developed, that time may not be far-fetched.

Having settled that it is to be considered as a document, electronic evidence will be facing the same obstacles an ordinary written document would have to hurdle. There are the questions relating to its admissibility including its authenticity, due execution, the best evidence rule, the parol evidence rule, and hearsay. Finally, the matter of its evidential weight will now be addressed.

---

[163] RULES OF COURT, Rule 130, sec. 1.

[164] RULES OF COURT, Rule 130, sec. 2.

[165] 1 RICARDO J. FRANCISCO, PLEADINGS AND TRIAL PRACTICE 353 (1977).

[166] Rep. Act No. 8792(2000), sec. 7, penultimate paragraph.

3. Authenticity and Due Execution

When one says that a document is authentic, what is meant is "that the document is not spurious, counterfeit, or of different import on its face from the one executed by the party, or that the party whose signature it bears gas signed it and that at the time it was signed it was in words and figures as set out in the pleadings."[167] Meanwhile, by due execution it is meant "that the document was signed voluntarily and knowingly by the party whose signature appears thereon, that if signed by somebody else such representative had the authority to do so, that it was duly delivered, and that the formalities were complied with."[168]

Of course the best way to prove the authenticity and due execution of a document is for all parties and witnesses to that particular document to admit its authenticity and due execution. But that would be wishing for the stars. The precise reason why these rules of evidence come into play is the existence of a controversy. People do not see eye to eye. More often than not, one side will be alleging that the document was forged and/or was not duly executed, contrary to the claim of the other side.

The solution to such a standoff is the institutionalization of an entity that would do for electronic documents and data messages what the notary public has done for written documents for centuries now. Some people call this entity a Certification Authority, others term it a trusted-third party, while some prefer CyberNotary. No matter what is it called, if something like the notary public is institutionalized to serve the peculiar needs of an electronic document or data message, then most of the problems about authenticity and due execution would be eradicated.

As aptly observed by one author:

> A primary problem with electronic commerce is that parties cannot physically verify with whom they are dealing. Thus, it is necessary for a trusted impartial third party called a Certification Authority (CA) to perform this function of identification. A CA can prevent disputes as to what actually occurred between two parties as well as prevent fraud and forgery. While the functions of a CA are similar to a notary, a CA is different because a CA is not physically present when the transaction was consummated.[169]

---

[167] 1 FLORENZ D. REGALADO, REMEDIAL LAW COMPENDIUM 155 (2000).

[168] *Id.* at 155-156.

[169] D. L. Gripman, *Electronic Document Certification: A Primer on the Technology Behind Digital Signatures*, 17 JOURNAL OF COMPUTER & INFORMATION LAW 769, 770-771 (1999).

It is quite amusing to note that humanity is now on the threshold of experiencing a similar problem it has encountered centuries ago (that of authenticating documents) and the solution lies in essentially the same institution (the notary). As recounted by the same author:

> The origins of the notary date back to the Roman Empire where the ability to read and write was not widespread. The notary was viewed as a trusted public official who for a fee, drafted and safeguarded documents (e.g., contracts) for the public record. Since then, the notary has become an essential part of modern business transactions. xxx However, all notaries have the authority to administer oaths and to attest to the authenticity of signatures on documents. This latter authority is one of the primary reasons the notary is essential to many business transactions. When a notary attests to the authenticity of a document by notarizing that document, the notary is verifying both the signature on the document and the signer's identity. Thus, a third party can reasonably rely on the notarization as indicating that the person who signed the document is who he or she claims to be.[170]

As discussed above,[171] it is advisable to institutionalize the CyberNotary, trusted third party or certification authority, whatever one may be inclined to call it. It is heartwarming to note that the Philippine Supreme Court is set to promulgate rules on "digital notarization."[172]

4. Best Evidence Rule

Under the present formulation of the rules on procedure, the original of a document is "one the contents of which are the subject of inquiry." Or "[w]hen a document is in two or more copies executed at or about the same time, with identical contents, all such copies are equally regarded as originals." Finally, "[w]hen an entry is repeated in the regular course of business, one being copied from another at or near the time of the transaction, all the entries are likewise regarded as originals."[173] The three kinds of original documents are bound by the tie that each of the three represent the "medium on which the information was fixed for the first time."[174] Hence, if the definition of the Rules of Court would not be changed then it would be "impossible to speak of 'original' data messages, since the addressee of a data message would always receive a copy thereof."[175] Thus, the lawmakers were constrained to modify the definition of an original document when it comes to electronic document or data message. The law reads:

---

[170] *Id.* at 771-772.

[171] See discussion on VI. Case in Point: Law of Contracts, *supra*.

[172] *SC to amend rules to boost RP e-commerce*, *supra* note 150.

[173] RULES OF COURT, Rule 130, sec. 4.

[174] UNCITRAL Guide to Enactment of the Model Law, *supra*. note 28, at par. 72.

[175] *Ibid.*

> (1) Where the law requires information to be presented or retained in its original form, that requirement is met by an electronic data message or electronic document if: the integrity of the information from the time when it was first generated in its final form, as an electronic data message or electronic document is shown by evidence *aliunde* or otherwise; and where it is required that information be presented, that the information is capable of being displayed to the person to whom it is to be presented.
>
> (2) Paragraph (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 purposes of subparagraph (a) of paragraph (1): 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 arises in the normal course of communication, storage and display; and 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 relevant circumstances.[176]

As correctly observed by Sen. Roco during the debate on the enactment of the law, a document produced by a computer is considered original regardless of the location where either party to the agreement downloads it.

With the progressive use of electronic documents, there will be a paradigmatic shift in the appreciation of whether a document is original or not for purposes of the best evidence rule. Unlike in the case of written on paper documents where the focus would be on the document itself, the focus of attention in the determination of the originality of an electronic document or data message would be on the integrity of the process involved in the generation of the electronic document or data message. In this regard, the same problems and solutions relating to the authenticity of the electronic document or data message would crop up.

5. Parol Evidence Rule

During the period for amendments, Senator Defensor Santiago asked if the second part of Section 8 of S.B. 1902 (now Section 6 of R.A.8792) would not create an exception to the parol evidence rule (Sec. 9, Rule 130 of the Rules of Court). In response, Senator Roco expressed the opinion that the parol evidence rule would be modified only with respect to the submission of a document downloaded from a computer. The senator went on to express the view that the rule on parol evidence would not be modified by Section 8 (now Section 6) because in court, when someone introduces something as reference, even if it is not fully reproduced, it is

---

[176] Rep. Act No. 8792 (2000), sec. 10.

still considered as part of the document which, according to the rule, cannot be modified. He noted that the document, being a data message, speaks for itself (making it appear that even the senators were confused by the rule on incorporation by reference). Asked by Senator Guingona to clarify the meaning of "incorporation by reference," Senator Roco explained that the data message can refer to a document that contains the description and details of a product being sold, and such incorporation by reference is valid.[177]

It is submitted that despite Sen. Roco's assurances, the rule on "incorporation by reference" will pose problems in its practical application considering that most documents incorporated by reference are long and in legal gobbledygook and most documents incorporating other documents are in the nature of adhesion contracts.

Thus, it must be doubly made sure that for the rationale behind the parol evidence rule to remain alive, that measures be taken so that the adhering party is truly informed and intelligently notified of the incorporated documents. "The fulfillment by the stronger party of the positive duty of information creates a presumption that the weaker party has knowledge of the substance of the incorporated terms. Courts are generally satisfied if the principal contractual document includes an express clause referencing the annexed document and, if that document is not given to the weaker party, such document is easily accessible to the weaker party."[178]

Minimum standards to regulate hypertext linking must be set. The font size must be big enough and placed in conspicuous part of the electronic document. It should not be put in fine print and at the bottom or the fringes of the electronic document, as what is being done know. Also, it must be made clear in the referencing text, without need of going to the referred text, that the referred text is part and parcel of the electronic document. There must be a sign and warning to that effect. For only "[w]hen a reference clause is clear, conspicuous, and precise, will [it] likely satisfy legislative and judicial requirements as to knowledge, including in particular the requirement of 'notice.'"[179]

6. The Hearsay Objection

A plausible objection to the presentation of a computer printout of an electronic document or data message is that the printout is hearsay unless all the persons who took part in the creation of the electronic document (from the

---

[177] Comm. Rpt No. 179, *supra* note 3, 76th Sess. (2000).
[178] LAROSE, *op. cit. supra* note 158 at 298.
[179] *Ibid.*

encoding to the storing to the printing as well as those that maintain the computer system containing the said document) are asked to authenticate the said computer printout.

Without these authenticating persons, the printout may indeed be considered hearsay. If only the encoder was presented to authenticate the document, he has no personal knowledge as to what happened to the electronic document from the time he encoded up to the time the computer printout was generated. His personal knowledge would only be limited to his act of encoding.

The rationale behind this exclusion due to hearsay is that "the party against whom [the hearsay evidence] is presented is deprived of his right and opportunity to cross-examine the persons to whom the statements or writings are attributed."[180]

However, for computer-printouts made in the ordinary course of business, there is a refuge from the hearsay attack, that is, the business records exception rule. Under this rule, it is provided that in "the presentation and admission as evidence of entries made in the regular course of business, there is no overriding necessity to bring into court all the clerks or employees who individually made the entries in a long account; it is sufficient that the person who supervises the work of the clerks or other employees making the entries testify that the account was prepared under his supervision and that the entries were regularly entered in the ordinary course of business."[181]

The business records exception is "warranted by the necessity for such evidence and/or on the assumption that, in the ordinary course of events, the same are trustworthy."[182] The practical necessity factor is buttressed by the fact that "each business transaction often involves separate stages and parties, no one person can fully testify as to the entire transaction."[183] And the records are presumptively trustworthy "because they are based upon reports made by persons who are under a routine duty to record them."[184]

Thus in various cases in the United States, computer printouts have successfully offered and admitted as evidence under the business exception rule. It

---

[180] 2 REGALADO, *supra* note 154 at 486.

[181] *Id.* at 498.

[182] *Id.* at 486.

[183] J. R. KAHN, IMPLICATIONS OF COMPUTER TECHNOLOGY AND USE FOR THE LAW OF EVIDENCE (1989).

[184] *Ibid.*

suffices that proper foundation be laid that (1) the printout was made in the ordinary course of business[185] and (2) the process that generated the printout was reliable.[186]

In establishing the proper foundation for the business records exception, it has been held that it is not necessary that the person who caused computer printouts to be produced be the same person who had fed the original data into the computer.[187] It would also suffice if the person responsible for record keeping identified the printouts as originals.[188] More importantly, the witness laying the basis for the computer printout need not be a computer programmer.[189]

And as far as the computer system is concerned, it has likewise been held that the computer need not be tested for programming errors.[190] Also, the proponent of the computer printout need not prove that the acceptability of hardware and software of the computer system as well as the internal maintenance and accuracy checks used on the said system.[191]

The E-Commerce Act has codified this hearsay exception by allowing proof as to admissibility via an affidavit to the best of the deponent's knowledge. In this regard, the law provides that:

> The matters referred to in Section 12, on admissibility and Section 9, on the presumption of integrity, may be presumed to have been established by an affidavit given to the best of the deponent's knowledge subject to the rights of parties in interest as defined in the following section.[192]

7. Evidentiary Weight

In the proper assessment of the evidentiary weight of a particular piece of electronic evidence, the law provides that:

> In assessing the evidential weight of an electronic data message or electronic document, the reliability of the manner in which it was generated, stored or

---

[185] WGNX, Inc. v. Gorham, 364 S.E.2d 621, 185 Ga.App. 489 [1988]; Smolen v. Dahlman Apartments, Ltd., 463 N.W..2d 261, 186 Mich.App. 292 [1990]; Needham v. New Jersey Ins. Underwriting Ass'n, 553 A.2d 821, 230 N.J.Super. 358 [1989].

[186] Weisman v. Hopf-Himsel, Inc., 535 N.E.2d 1222 [1989]; Prudential Ins. Co. of America v. Kinney Plantation, Inc., 489 So.2d 1211 [1986]; U.S. v. Duncan, 30 M.J. 1284 [1990].

[187] Briar Hill Apartments v. Teperman, 568 N.Y.2d 50, 165 A.D.2d 519 [1991].

[188] Borton v. State, 563 N.E.2d 182 [1990].

[189] U.S. v. Linn, 880 F.2d 209 [1989].

[190] U.S. v. Moore, 923 F.2d 910 [1991].

[191] People v. Lugashi. 252 Cal.Rprtr. 434, 205 C.A.3d 632 [1988].

[192] Rep. Act No. 8792 (2000), sec. 14.

> communicated, the reliability of the manner in which its originator was identified, and other relevant factors shall be given due regard.[193]

Such a standard is only proper considering that it is "in accord with the common knowledge and experience of mankind."[194] Only an electronic document generated, stored or communicated in a reliable manner can be of satisfactory use as evidence.

The problem with use of reliability as the barometer for evidential weight is that the same standard is also used by the law to determine admissibility, to wit:

> Electronic documents shall have the legal effect, validity or enforceability as any other document or legal writing, and -
>
> (a) Where the law requires a document to be in writing, that requirement is met by an electronic document if the said electronic document maintains its integrity and reliability and can be authenticated so as to be usable for subsequent reference, in that -
>
> The electronic document has remained complete and unaltered, apart from the addition of any endorsement and any authorized change, or any change which arises in the normal course of communication, storage and display; and
>
> The electronic document is reliable in the light of the purpose for which it was generated and in the light of all the relevant circumstances.[195]

It is submitted that there was no more need to put reliability as one of the criteria for admissibility. It is enough that reliability is the gauge of the evidentiary weight. But, instead, the law envisages a situation where one criterion will be used twice, once for admissibility and another for weight.

The probable reason behind this is the sense of untrustworthiness one might have for electronic documents considering that it is generally accepted to be easily changed and fabricated. However, the facility of fabrication could be argued to be the same as for written paper documents and for electronic documents, at least for the determined forger. Thus, to actually give life to the law's intent to put electronic documents and data messages in the same plane as written paper documents, it is humbly submitted that the test of reliability be used only for the purpose of determining evidential weight.

---

[193] Rep. Act No. 8792 (2000), sec. 12, last paragraph.
[194] 2 REGALADO, *op. cit. supra* note 154 at 553.
[195] Rep. Act No. 8792 (2000), sec. 7.

As aptly observed by one British lawyer:

> It would seem perfectly feasible that where there are doubts as to the reliability of computer-generated evidence these doubts should not go to the issue of admissibility but rather to the weight of the evidence. xxx Paper based records are also susceptible to alteration and deterioration yet, where it is alleged that such alteration has taken place, the paper document remains admissible and the challenge goes to the question of its weight as evidence, to be decided on the basis of the evidence called to prove falsification or authentication.[196]

Thus, as far as evidentiary weight is concerned, one need not be overly concerned with computer-generated evidence.

VIII. CONCLUSION

The Electronic Commerce Act of 2000 is a revolutionary piece of legislation, not only in the light of high technology subject matter and wide spread impact on Philippine Law, but more so because of the manner and motivation behind its enactment. It is, in a very literal sense, an example of international legislation incorporated into our law. Both the motivation (global competitiveness) and the source (the UNCITRAL Model law on E-Commerce) were international in character.

In enacting R.A. 8792 in the way it did, the legislature appears to be betting that by grafting cutting edge, albeit unfamiliar, piece international legislation onto the body of Philippine Law it can successfully push the Philippine economy into a sucessful CyberHub overnight. The gamble appears to be that providing what has internationally been determined to be the ideal legal will be sufficient to whatever obstacles exist in terms of physical infrastructure, experience and expertise.

Will the gamble pay off? Is it possible to successfully put the cart before the horse? Only time will tell. In the meantime, the Act has without a doubt unleashed a Pandora's box of questions as to its proper interpretation and application that will keep practitioners and courts engrossed in the brave new world of electronic data and electronic documents for some time come.

-o0o-

[196] A. Hoey, *Analysis of The Police and Criminal Evidence Act, s. 69 – Computer Generated Evidence*, WEB JOURNAL OF CURRENT LEGAL ISSUES (1996).