

THE ELECTRONIC COMMERCE ACT (R.A. 8792)
AN OVERVIEW OF IT'S (INFORMATION TECHNOLOGY)
IMPACT ON THE PHILIPPINE LEGAL SYSTEM

JOAN M. PADILLA*

I. INTRODUCTION

In this age of computers and IT (information technology), the medium of the internet and other electronic means of interchange are used worldwide for various undertakings – both commercial and non-commercial. This rapid development of information and communication technologies and the growing number of transactions accomplished through electronic means necessitated the passage of a law that would facilitate and regulate these electronic transactions – the Electronic Commerce Act.

Republic Act No. 8792 is the merged version of House Bill No. 9971 and Senate Bill No. 1902. It was signed into law on June 14, 2000. “A month later or on July 14, 2000, the Implementing Rules and Regulations (IRR) was digitally signed by Secretaries Manuel A. Roxas II (DTI) and Benjamin E. Diokno (DBM) and Governor Rafael B. Buenaventura (BSP) during the plenary session of the Global Information Infrastructure Commission’s (“GIIC”) Asia Regional Conference held in Makati City, Manila.”¹

* '06 LI.B., cand., University of Santo Tomas Faculty of Civil Law; Business Manager, UST Law Review

¹ ATTY. JESUS M. DISINI, JR., THE ELECTRONIC COMMERCE ACT AND ITS IMPLEMENTING RULES AND REGULATIONS, <http://www.disini.ph/downloads/EcomIRR%20Annotation.pdf> (last accessed Jan 06, 2006).

Thereafter, acting on the Memorandum dated 18 June 2001 of the Committee on the Revision of the Rules of Court to Draft the Rules on E-Commerce Law, the Supreme Court issued A.M. No. 01-7-01-SC (Rules on Electronic Evidence) which took effect on August 1, 2001.²

This Act is basically patterned from United Nations Commission on International Trade Law (UNCITRAL) Model Law on Electronic Commerce to maintain uniformity and harmony with the other member-states of the United Nations. Being global by nature, there is a need for international coordination and harmonization of the government policies affecting electronic commerce.

The salient features of the Act are:

- ← It provides for the legal recognition of electronic documents or data messages;
- ← It provides for the legal recognition of electronic signatures;
- ← It provides for the legal recognition of electronic contracts;
- ← It mandates all government agencies to, among others, transact government business and perform government functions using electronic data messages or electronic documents within two (2) years from the date of effectivity of the Act;
- ← It mandates the government to install an electronic network to known as the RPWeb within two years (2) years from the date of effectivity of the Act; and
- ← It penalizes the offenses of hacking and piracy.

The primary objective of the Act is to provide a secure legal framework and environment for electronic commerce.³ It seeks to protect the integrity of electronic documents and electronic signatures as well as its transmission and communication so as to build and ensure the trust and reliance of the public on electronic transactions. Section 3 of RA 8792 provides that “the Act aims to facilitate domestic and international dealings, transactions, arrangements, agreements, contracts and exchanges

² A.M. No. 01-7-01-SC.- RE: RULES ON ELECTRONIC EVIDENCE

³ DISINI, *supra* note 1, at 8.

and storage of information through the utilization of electronic, optical and similar medium, mode, instrumentality and technology, to recognize the authenticity and reliability of electronic documents related to such activities and to promote the universal use of electronic transactions in the government and by the general public.”⁴

Despite these laudable aims and objectives, many are still skeptical on the methods provided under the law to ensure the integrity and security of these electronic transactions. Most of them question the admissibility and weight given to electronic evidence, its authenticity and integrity as well as the manner used to verify the same, and the impact of its legal recognition on the Philippine legal system.

II. ELECTRONIC COMMERCE IN GENERAL

Electronic Commerce is defined as the process of buying and selling goods electronically by consumers and from company to company through computerized business transactions.⁵ The Organization for Electronic Cooperation and Development defines it as “commercial transactions based on electronic transmission of data over communication networks such as the Internet.”⁶ Although the definition of electronic commerce is strictly confined to commercial undertakings, RA 8792 is made applicable to both commercial and non-commercial transactions.

To have a better understanding of the E-Commerce Act, there is a need to define three very important terms – *electronic data messages*, *electronic document* and *electronic signature*. These terms are given the functional equivalent of their paper-based counterparts upon compliance with the requirements of the Electronic Commerce Act. Such legal recognition is relevant in facilitating electronic transactions.

⁴ An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions, Penalties for Unlawful Use thereof, and Other Purposes, Republic Act No. 8792, § 3 (2000)

⁵ G. SY, ELECTRONIC COMMERCE ACT 73 (2001)

⁶ *id.* at 56

Section 6(e) of the IRR defines *electronic data messages* as referring to “information generated, sent, received or stored by electronic, optical or similar means, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy.”⁷ An *electronic document*,” on the other hand, is defined under subsection (h) of the same section as an “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.”⁸ The Rules further provide that the term “*electronic document*” shall be equivalent to and be used interchangeably with “*electronic data message* and vice versa.

Simply put, an electronic data message or electronic document is any electronic file providing information that is generated, sent, received or stored by electronic, optical or similar means.

- ← “*Generated by electronic means*” – This includes word processing and other computer files, electronic mail, SMS (short message service) messages, and other documents which are created through electronic devices.
- ← “*Sent or Received by electronic means*” – Since only the mode of transmission is relevant, the output generated can now be considered an electronic data message. In other words, a fax, telegram, or telex message would be included because these were transmitted through telecommunications networks – as would transaction receipts for credit card, debit card, ATM card and other similar point of sale transactions.
- ← “*Stored by electronic means*” – This contemplates a situation where the electronic data is not sent by the creator thereof but merely stored. It necessarily includes computer files which are not intended for transmission but mere storage. This likewise refers to situations where paper documents are transformed into paperless form by digital imaging or scanning. What was once a paper document is now

⁷ IMPLEMENTING RULES AND REGULATIONS OF REPUBLIC ACT NO. 8792

⁸ *id.* at §6(h)

transformed into an electronic data message even though its final destination is an optical CD-ROM disk. It is submitted that the output of devices directly connected to computers are electronic data messages. These will include print outs from such devices as laser, inkjet, and dot-matrix printers. These are undeniably paper documents and seem to be excluded from the definition of electronic data messages. But what cannot be denied is that such electronic data messages are either generated or stored by electronic means.”⁹

Finally, an “*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”.¹⁰ In other words, an electronic signature is any mark in electronic form used to identify a person and to show his intention of approving and authenticating an electronic document.

III. LEGAL RECOGNITION OF ELECTRONIC DATA MESSAGES AND ELECTRONIC DOCUMENTS

It is a fundamental principle under this law that electronic documents are given the functional equivalent or the same legal status as their paper-based counterparts. That is why Section 7 of the IRR provides that:

“Information shall not be denied validity or enforceability solely on the ground that it is in the form of an electronic data message or electronic document, purporting to give rise to such legal effect. *Electronic data messages or electronic documents shall have the legal effect, validity or enforceability as any other document or legal writing.* In particular, subject to the provisions of the Act and these Rules:

⁹ DISINI, *supra* note 1, at 11.

¹⁰ *Supra* note 7

(a) A requirement under law that information is in writing is satisfied if the information is in the form of an electronic data message or electronic document.

(b) 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.

(c) A requirement under law for a person to provide information to another person in a specified non-electronic form is satisfied by the provision of the information in an electronic data message or electronic document if the information is provided in the same or substantially the same form.

(d) Nothing limits the operation of any requirement under law for information to be posted or displayed in specified manner, time or location; or for any information or document to be communicated by a specified method unless and until a functional equivalent shall have been developed, installed, and implemented.”¹¹ (emphasis supplied)

In sum, this section provides that electronic documents shall have the same legal effect, validity and enforceability as any other document or legal writing. This means that an electronic document would be sufficient in compliance with the requirements in some laws that the act, transaction, event or agreement be in writing for its validity and/or enforceability. Among such laws are:

1. Article 1356 of the Civil Code (Contracts)
2. Article 1403, paragraph 2 and Article 1405 of the Civil Code (Statute of Frauds)
3. Article 1356 to 67 of the Civil Code (Reformation of Instruments)
4. Negotiable Instruments Law
5. Rule 130, Section 2, 3 and 4 of the Rules of Court (Best Evidence Rule)
6. Rule 132, Section 24 of the Rules of Court

¹¹ *Supra* Note 7

However, before the electronic document can be regarded a “writing” under RA 8792, it must comply with the requirements under Section 10 of the IRR which provides that:

“Section 10. *Writing*. – Where the law requires a document to be in writing, or obliges the parties to conform to a writing, or provides consequences in the event information is not presented or retained in its original form, an electronic document or electronic data message will be sufficient if the latter:

(a) maintains its integrity and reliability; and
(b) can be authenticated so as to be usable for subsequent reference, in that:

(i) It 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

(ii) It is reliable in the light of the purpose for which it was generated and in the light of all relevant circumstances.”¹²

If the electronic document does not satisfy the requirements of Section 10 then it will not be given the same status as a “written” document. Despite the same, however, the contents of which may still be admissible in evidence as “proof” thereof.

But the mere fact that the electronic document can be considered as a “writing” does not mean that it can also be given the legal recognition of an “original document.” A distinction must be made between a “writing” and an “original” electronic document.

“Original electronic documents are legally relevant and significant only if they retain their uniqueness. The presentation of the physical document itself establishes the right of the holder and his authority to perform transactions relating to them. Hence, the integrity of the “original” must be established before it can be considered as such. Otherwise, the

¹² *Id.* at §10

faith in and commercial reliance upon such documents in electronic form might be eroded.”¹³

Section 11 of the IRR provides that “where the law requires that a document be presented or retained in its original form, that requirement is met by an electronic document or electronic data message if:

(a) There exists a reliable assurance as to the integrity of the electronic document or electronic data message from the time when it was first generated in its final form and such integrity is shown by evidence aliunde (that is, evidence other than the electronic data message itself) or otherwise; and

(b) The electronic document or electronic data message is capable of being displayed to the person to whom it is to be presented.

(c) For the purposes of paragraph (a) above:

(i) 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

(ii) 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.

An electronic data message or electronic document meeting and complying with the requirements of Sections 6 or 7 of the Act shall be the best evidence of the agreement and transaction contained therein.

The standard for integrity of “original” electronic documents is different from that of electronic “writings.” As above-stated, *the integrity of an “original” must be shown to exist “from the time when it was first generated in its final form and it must be shown by evidence aliunde.”* Moreover, the criteria for assessing its integrity is whether it can be shown that the information remained complete and unaltered from the time it

¹³ DISINI, *supra* note 1, at 16.

was generated in its final form. This was interpreted by Atty. Jesus M. Disini Jr., in his annotations on the Implementing Rules and Regulations of RA 8792, to mean that “the Act also intended to include a situation where the document was first composed on paper and later transferred to a computer and not merely from the time it was translated into electronic form.”¹⁴

If the electronic document meets the requirements of an “original” under Section 11 then it can also be considered as an original document in contemplation of the Best Evidence Rule which provides that “*when the subject of the inquiry is the contents of a document, no evidence shall be admissible other than the original document itself.*”¹⁵ Moreover, Rule 4 Section 1 of the Rules on Electronic Evidence also provides that “an electronic document shall be regarded as the equivalent of an original document under the Best Evidence Rule if it is a printout or output readable by sight or other means, shown to reflect the data accurately.”¹⁶

Although the final paragraph of Section 11 provides that “electronic data messages and electronic documents meeting and complying with the requirements of Sections 6 or 7 of the Act shall be the best evidence of the agreement and transaction contained therein,”¹⁷ it does not mean that we can forego with the requirement of Section 10 and 11 of the IRR requiring proof of their integrity and authenticity. “While an electronic data message is *by itself* the best evidence, it must still independently qualify as being either a “writing” or an “original” under Sections 11 and 12 of the IRR, respectively. In the case of the latter documents, evidence of reliability and integrity must also be presented. Otherwise, the electronic data message or document will merely be taken as evidence of its contents but not be considered a “writing” or an “original” under Philippine law.”¹⁸

¹⁴ *id.*

¹⁵ RULES OF COURT, RULE 130, § 3

¹⁶ *Supra* note 2

¹⁷ *Supra* note 7

¹⁸ DISINI, *supra* note 1, at 16.

IV. MODES FOR ESTABLISHING INTEGRITY AND AUTHENTICATION

As earlier discussed, to independently qualify as a “writing” or an “original” under RA 8792, the electronic document must first show proof of its integrity, reliability and authenticity. To establish its authenticity, Section 2 Rule 5 of the Rules on Electronic Evidence provides that:

“SEC. 2. *Manner of authentication.* – Before any private electronic document offered as authentic is received in evidence, its authenticity must be proved by any of the following means:

(a) by evidence that it had been digitally signed by the person purported to have signed the same;

(b) by evidence that other appropriate security procedures or devices as may be authorized by the Supreme Court or by law for authentication of electronic documents were applied to the document; or

(c) by other evidence showing its integrity and reliability to the satisfaction of the judge.”¹⁹

In relation thereto, Section 15 of the IRR provides that:

“Section 15. *Method of Authenticating Electronic Documents, Electronic Data Messages, and Electronic Signatures.* – Electronic documents, electronic data messages and electronic signatures, shall be authenticated by demonstrating, substantiating and validating a claimed identity of a user, device, or another entity in an information or communication system.

Until the Supreme Court, by appropriate rules, shall have so provided, electronic documents, electronic data messages and electronic signatures, shall be authenticated, among other ways, in the following manner:

(a) The electronic signature shall be authenticated by proof that a letter, character, number or other symbol in electronic form representing the persons named in and attached to or logically associated with an electronic data message, electronic document,

¹⁹ *Supra* note 2

or that the appropriate methodology or security procedures, when applicable, were 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;

(b) The electronic data message or electronic document shall be authenticated by proof that an appropriate security procedure, when applicable was adopted and employed for the purpose of verifying the originator of an electronic data message or electronic document, or detecting error or alteration in the communication, content or storage of an electronic document or electronic data message from a specific point, which, using algorithm or codes, identifying words or numbers, encryptions, answers back or acknowledgement procedures, or similar security devices.²⁰

As to the method to be used in establishing the integrity of electronic documents, Section 17 of the IRR provides that:

In the absence of evidence to the contrary, the integrity of the information and communication system in which an electronic data message or electronic document is recorded or stored may be established in any legal proceeding, among other methods:

(a) By evidence that at all material times the information and communication system or other similar device was operating in a manner that did not affect the integrity of the electronic document or electronic data message, and there are no other reasonable grounds to doubt the integrity of the information and communication system;

(b) By showing that the electronic document or electronic data message was recorded or stored by a party to the proceedings who is adverse in interest to the party using it; or

(c) By showing that the electronic document or electronic data message was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not act under the control of the party using the record."²¹

²⁰ *Supra* note 7

²¹ *Id.*

V. LEGAL RECOGNITION OF ELECTRONIC SIGNATURES

As stated earlier, an electronic signature is any mark in electronic form used to identify a person and to show his intention of approving and authenticating an electronic document. Because it is given the functional equivalent of a handwritten signature, RA 8792 imposes strict requirements before it can be classified as such. Section 13 of the IRR provides that:

An electronic signature relating to an electronic document or electronic data message shall be equivalent to the signature of a person on a written document if the signature:

(a) "is an electronic signature as defined in Section 6(g) of these Rules; and

(b) is proved by showing that a prescribed procedure, not alterable by the parties interested in the electronic document or electronic data message, existed under which:

(i) A method is used to identify the party sought to be bound and to indicate said party's access to the electronic document or electronic data message necessary for his consent or approval through the electronic signature;

(ii) Said method is reliable and appropriate for the purpose for which the electronic document or electronic data message was generated or communicated, in the light of all circumstances, including any relevant agreement;

(iii) 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,

(iv) 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.

The parties may agree to adopt supplementary or alternative procedures provided that the requirements of paragraph (b) are complied with".²²

²² *Supra* note 7

Moreover, to establish the authenticity of the electronic signature Section 2 of Rule 4 of the Rules on Electronic Evidence provides that:

“An electronic signature may be authenticated in any of the following manner:

- (a) By evidence that a method or process was utilized to establish a digital signature and verify the same;
- (b) By any other means provided by law; or
- (c) By any other means satisfactory to the judge as establishing the genuineness of the electronic signature.”²³

These stringent requirements were precisely imposed to ensure the integrity and reliability of these electronic signatures. And it is only upon proof of its authentication that this electronic signature will enjoy the following presumptions:

“Section 14. *Presumption Relating to Electronic Signatures.* – In any proceeding involving an electronic signature, the proof of the electronic signature shall give rise to the rebuttable presumption 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 data message or electronic document unless the person relying on the electronically signed electronic data message or 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.”²⁴

“SEC. 3. *Disputable presumptions in relation to electronic signature.* – Upon the authentication of an electronic signature, it shall be presumed that:

- (a) The electronic signature is that of the person to whom it correlates;

²³ *Supra* note 2

²⁴ *Supra* note 7

(b) The electronic signature was affixed by that person with the intention of authenticating or approving the electronic document to which it is related or to indicate such person's consent to the transaction embodied therein; and

(c) The methods or processes utilized to affix or verify the electronic signature operated without error or fault."²⁵

VI. ADMISSIBILITY AND EVIDENTIAL WEIGHT

Section 3, Rule 128 of the Rules of Court provides that "evidence is admissible when it is relevant to the issue and is not excluded by Law or these Rules."²⁶ In other words, the evidence is admissible when it is both relevant and competent. On the other hand, the evidentiary weight to be given to the evidence will depend on its probative value or the sufficiency thereof.

As previously stated, one of the salient features of the E-Commerce Act is that electronic documents, electronic signatures and even electronic contracts shall be given the functional equivalent of their paper-based counterparts. Corollary thereto, Section 18 of the IRR provides that "in any legal proceeding, nothing in the application of the rules on evidence shall deny the admissibility of an electronic data message or electronic document in evidence:

- (a) On the sole ground that it is in electronic form; or
- (b) On the ground that it is not in the standard written form."²⁷

It further 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 communicated, the reliability of the manner in which its originator was identified, and other relevant factors shall be given due regard."²⁸

²⁵ *Supra* note 2

²⁶ REVISED RULES ON EVIDENCE

²⁷ *Supra* note 7

²⁸ *Supra* note 7

Moreover, Section 1 Rule 7 of the Rules on Electronic Evidence provides that in assessing the evidentiary weight of an electronic document, the factors to be considered are:

“(a) The reliability of the manner or method in which it was generated, stored or communicated, including but not limited to input and output procedures, controls, tests and checks for accuracy and reliability of the electronic data message or document, in the light of all the circumstances as well as any relevant agreement;

(b) The reliability of the manner in which its originator was identified;

(c) The integrity of the information and communication system in which it is recorded or stored, including but not limited to the hardware and computer programs or software used as well as programming errors;

(d) The familiarity of the witness or the person who made the entry with the communication and information system;

(e) The nature and quality of the information which went into the communication and information system upon which the electronic data message or electronic document was based; or

(f) Other factors which the court may consider as affecting the accuracy or integrity of the electronic document or electronic data message.”²⁹

However, it is only upon compliance with the Rules establishing the integrity and authenticity of these electronic documents and electronic signatures may we then consider the admissibility and evidentiary weight given to them by the law. This is to further ensure the security and reliability of these electronic evidence as means of facilitating commercial and non-commercial transactions.

²⁹ *Supra* note 2

VII. IMPACT ON THE PHILIPPINE LEGAL SYSTEM

The provisions of the Act giving legal recognition to electronic documents, electronic signatures and other electronic evidence and the admissibility and evidentiary weight given to them as the functional equivalent of their paper-based counterparts modified significantly – the Rules on Evidence and Contract Laws.

Article 1356 of the Civil Code provides that “contracts shall be obligatory, in whatever form they may have been entered into, provided all the essential requisites for their validity are present. However, when the law requires that a contract be in some form in order that it may be valid and enforceable, or that a contract be proved in a certain way, that requirement is absolute and indispensable.”³⁰

Although as a general rule, a contract is valid in whatever form it may be. There are certain laws which require that the agreement be embodied in a specific form, e.g. in writing, either for its validity and/or enforceability. Among such laws are:

1. Article 1403, paragraph 2 and Article 1405 of the Civil Code (Statute of Frauds)
2. Donations of personal property with value in excess of 5,000 pesos (Art. 748 of the Civil Code)
3. Contract of Antichresis where the amount of the principal and interest must be in writing (Art. 2134 of the Civil Code)
4. Stipulations to pay interest on loans (Art. 1956 of the Civil Code)
5. Power of Attorney to sell land or any interest therein (Art. 1874 of the Civil Code)
6. Stipulations limiting a common carriers liability to less than extraordinary diligence (Art. 1744 of the Civil Code)
7. Marriage Settlements (Art. 77 of the Family Code)
8. Assignment of Copyright in whole or in part during the lifetime of the author (Sec. 180.2 of the Intellectual Property Code)

³⁰ CIVIL CODE, art. 1356

With the passage of the RA 8792, the requirement under the above-mentioned laws that the agreement be embodied in writing either for its validity and/or enforceability is satisfied if such agreement is embodied in electronic form.

Moreover, the Electronic Commerce Act explicitly validated the recognition of electronic contracts in the Philippines.

Section 21. *Formation and Validity of Electronic Contracts.*

Except as otherwise agreed by the parties, an offer, the acceptance of an offer and such other elements required under existing laws for the formation and perfection of contracts may be expressed in, demonstrated and proved by means of electronic data message or electronic documents and no contract shall be denied validity or enforceability on the sole ground that it is in the form of an electronic data message or electronic document, or that any or all of the elements required under existing laws for the formation of the contracts is expressed, demonstrated and proved by means of electronic documents.³¹

Corollary thereto, the Act and its IRR provided for the rules that will govern the attribution of electronic data message, agreement or acknowledgement of receipt of electronic documents, the time of dispatch and receipt of electronic documents and the place of dispatch and receipt thereof. These rules allow the use of electronic data messages or electronic documents in the formation of contracts.

On the other hand, the Rules on Electronic Evidence (drafted in consideration of the E-Commerce Act) modified notably the prevailing rules on evidence under the Rules of Court. Section 1, Rule 3 thereof states that “whenever a rule of evidence refers to the term of writing, document, record, instrument, memorandum or any other form of writing, such term shall be deemed to include an electronic document as defined in these Rules.”³² In addition thereto, it amended the Best

³¹ *Supra* note 7

³² *Supra* note 2

Evidence Rule in the Rules of Court by providing that “electronic documents shall be regarded as the equivalent of an original document under the Best Evidence Rule if it is printout or output readable by sight or other means, shown to reflect the data accurately.”³³

Another development is the recognition of the admissibility of text messages as evidence in court or other proceedings. In the recent case of *Zaldy Nuez v. Elvira Cruz Apao-Tinga*, the Supreme Court held that “the text messages were properly admitted by the Committee since the same are covered by Section 1(k), Rule 2 of the Rules on Electronic Evidence which states:

“Ephemeral electronic communication” refers to telephone conversations, text messages... and other electronic forms of communication the evidence of which is not recorded or retained.”

Under Section 2, Rule 11 of the Rules on Electronic Evidence, “Ephemeral electronic communications shall be proven by the testimony of a person who was a party to the same or who has personal knowledge thereof...”³⁴

Verily, the use of the internet, the Electronic Purchasing System (EPS), SMS and multi-media messaging and other electronic means of interchange have revolutionized business transactions and our everyday affairs. Such trend towards modernization and technological advancement necessitates knowledge and understanding of the E-Commerce Act. For there is indeed no doubt its passage has created a big impact on the Philippine legal system and our everyday lives.

³³ *id.*

³⁴ *Nuez v. Apao-Tinga*, A.M. No. CA-05-18-P, April 12, 2005