

THE ELECTRONIC COMMERCE ACT AND ITS IMPLEMENTING RULES AND REGULATIONS

Annotations by
Atty. Jesus M. Disini, Jr.
Legislative History by
Janette C. Toral

September 2000



PHILEXPORT

PHILIPPINE EXPORTERS CONFEDERATION, INC.

This material is published by the Philippine Exporters Confederation, Inc. (PHILEXPORT) to present various insights on a particular subject relevant to the export industry. The articles, papers, and other readings presented here were gathered from various sources and the views expressed do not necessarily reflect those of PHILEXPORT, USAID, or The TAPS Project.

Atty. Disini is Managing Partner in the law firm of Disini & Disini, and is the principal drafter of the Implementing Rules and Regulations of Republic Act 8792, otherwise known as the E-Commerce Law. Ms. Toral is the founder of the Philippine Internet Commerce Society and was actively involved in lobbying for the passage of the E-commerce Law.

The authors wish to acknowledge the use of materials prepared by Atty. Rodolfo Noel S. Quimbo on the Senate deliberation with respect to the Senate deliberation on Senate Bill 1523.

CONTENTS

Introduction

3

Declaration of Policy and Principles for Electronic Commerce Promotion

4

Electronic Commerce in General

10

Electronic Commerce in Carriage of Goods

28

Electronic Transactions in Government

31

Final Provisions

34

Republic Act No. 8792

Implementing Rules and Regulations of the Electronic Commerce Act

Annotations by
Atty. Jesus M. Disini, Jr.
Legislative History by
Janette C. Toral

Introduction.

The Electronic Commerce Act (Republic Act No. 8792; the “Act”) is by all means a significant piece of legislation for the Philippines. As intended, the passage of the Act has spurred investments in Information Technology projects and even a number of back-door listings in the Philippine Stock Exchange. Interest in electronic commerce is at an all-time high and companies have been forced to deal with the changes brought about by the New Economy.

It has been said, time and again, that in this new age, success will depend less upon the size of an organization but the speed by which it can implement its plan and take the first-mover advantage. Andy Grove of Intel has also been quoted as saying that in five years all companies will be Internet companies or not be companies at all. From all indications, the Act has had the effect of driving these ideas into local companies who have begun to examine themselves and their role in the New Economy.

It should be stressed that the passage of the Act is but the first step in the government’s efforts to secure the country’s place in the New Economy. Other contentious legal issues such as jurisdiction, digital signatures, intellectual property, privacy, consumer issues, domain names, and others, were intentionally excluded from the Act’s purview and rightly so. If Congress were to discuss these issues and attempt legislation, it might unduly delay the passage of the Act. Besides, many if not all of these issues remain unresolved even in developed countries. To discuss them would only result in the same deadlock seen elsewhere. More importantly, to delay the Act’s passage would be to deny meeting its express goal — the establishment of a secure legal framework for electronic commerce.

PART I

DECLARATION OF POLICY AND PRINCIPLES FOR ELECTRONIC COMMERCE PROMOTION

Chapter I - Declaration of Policy

Section 1. Declaration of Policy. The State recognizes the vital role of information and communications technology (ICT) in nation-building; the need to create an information-friendly environment which supports and ensures the availability, diversity and affordability of ICT products and services; the primary responsibility of the private sector in contributing investments and services in ICT; the need to develop, with appropriate training programs and institutional policy changes, human resources for the information age, a labor force skilled in the use of ICT and a population capable of operating and utilizing electronic appliances and computers; its obligation to facilitate the transfer and promotion of technology; to ensure network security, connectivity and neutrality of technology for the national benefit; and the need to marshal, organize and deploy national information infrastructures, comprising in both communications network and strategic information services, including their interconnection to the global information networks, with the necessary and appropriate legal, financial, diplomatic and technical framework, systems and facilities.

History of the Electronic Commerce Act. The Electronic Commerce Act (Republic Act No. 8792; the "Act") is the merged version of House Bill No. 9971 (HB 9971) and Senate Bills No. 1902 (SB 1902). The primary authors and sponsors were Sen. Ramon Magsaysay, Jr., Reps. Leandro Verceles, Jr. and Marcial Punzalan, Jr. Co-Authors of the Act who filed electronic commerce bills were Sens. Juan Flavio, and Blas Ople and Reps. Harry Angping, Roilo

Golez and Dante Liban. Other co-authors include Sen. Vicente Sotto III, Franklin Drilon, Francisco Tatad, Raul Roco, Aquilino Pimentel Jr., Miriam Defensor Santiago and Reps. Herminio Teves, Magtanggol **Guinigundo**, Rolando Sarmiento, Orlando Fua, Joey Salceda, Oscar Moreno, and Ignacio Bunye.

Senate Bills. This first bill on electronic commerce was filed in 1992. It was called the Electronic Data Interchange (EDI) bill and was re-filed as Senate Bill No. 10 (SB 10) during the 11th Congress. However, when the United Nations Commission on International Trade Law ("UNCITRAL") Model Law on Electronic Commerce ("Model Law") was adopted, the EDI bill was abandoned in favor of the Model Law framework. Besides, the EDI bill was considered technology-specific and if passed, might inadvertently promote the use of a declining technology, EDI. In addition, it was felt that given the long and tedious legislative process in the Philippines, a technology-neutral law would provide more stability inasmuch as it can adapt to and withstand advances in technology.

The Model Law was thus incorporated in Committee Report No. 34 and Senate Bill No. 1523 (SB 1523). In addition, the Electronic Transactions Act of Singapore ("ETA") was considered as suggested by several participants in the technical working group. The ETA, at that time, had just been passed in Singapore and it was believed that innovations in that statute would prove beneficial in the Philippine setting. After the conclusion of interpellations for SB 1523, the bill was referred back to the Committees on Trade and Industry and Science and Technology where it was replaced by SB 1902. SB 1902 departs from SB 1523 in that provisions of the ETA were minimized and the bill reverted back to the framework of the Model Law. This revision

was prompted by concerns that since the Philippine judicial system frequently adopts US case law, conflicting Singaporean jurisprudence on the ETA might unduly confuse the issues on what is already considered a complex area of the law.

It is significant to point out that all debates in the Senate respecting the Act referred to SB 1523 not SB 1902. Hence, for those interested in performing research on the Senate deliberations, they should refer to the discussions on SB 1523. SB 1902 was approved on April, 2000.

House Bills. Reps. Angping and Liban filed EDI Bills in the House in 1998. Rep. Golez likewise filed a bill which covered diverse areas such as copyright and cybercrimes, as well as EDI. When Committee Report No. 34 and SB 1523 were filed in the Senate, Reps. Punzalan and Verceles filed separate bills which were copies of SB 1523. In March, 2000, both bills were merged into HB 9971 which was presented and deliberated upon by the House in May 2000. HB 9971 was approved by the House on June 6, 2000.

Bicameral Conference Committee. The Bicameral Conference Committee, tasked with reconciling the provisions of HB 9971 and SB 1902, convened on June 7, 2000 in Manila Hotel. As a rule, any provision appearing in one version which does not appear in the other, is adopted in the final report. Interestingly enough, since HB 9971 did not abandon the provisions of the ETA (as distinguished by SB 1902), these found their way back to the final version of the Act. In the case of conflicting provisions in both HB 9971 and SB 1902, these were resolved through discussion. The report of the Bicameral Conference Committee was issued on June 7, 2000 and approved by the House later that evening. On June 8, 2000, the Senate approved the same report and the Act was referred to

the Office of the President for signing.

The Inter-Agency Task Force. The Electronic Commerce Act (Republic Act No. 8792; the "Act") was signed into law on June 14, 2000. On that day, an inter-agency task force convened for the purpose of drafting the Act's Implementing Rules and Regulations ("IRR"). The task force was co-chaired by the Department of Trade and Industry ("DTI"), Department of Budget and Management ("DBM"), and the Bangko Sentral ng Pilipinas ("BSP"). Representatives from the following government agencies likewise sat as members of the task force and participated in the deliberations: Commission on Audit ("COA"), Department of Science and Technology ("DOST"), Department of Transportation and Communications ("DOTC"), National Telecommunications Commission ("NTC"), Bureau of Internal Revenue ("BIR"), Intellectual Property Office ("IPO"), Bureau of Product Standards ("BPS"), National Development Corporation ("NDC"), Board of Investments ("BOI") and National Computer Center ("NCC"). Members of the private sector who provided their inputs were, among others: Ayala Corporation, Disini & Disini Law Office, Equitable Card Corporation, Globe Telecoms, Philippine Internet Commerce Society, SGV & Co. (Arthur Andersen), and the TAPS Project of PHILEXPORT and USAID.

The author drafted the IRR and presented the first version at the task force's second meeting on June 20, 2000. After collaborating on the draft IRR, the task force presented the same at a public hearing held at the Board of Investments on July 3, 2000. The task force assembled for the last time on July 4, 2000 to discuss the concerns raised at the public hearing and to settle pending issues leading to the final draft. Thereafter, the drafting of the IRR was coordinated by the DTI's Office of the

Secretary where only minor revisions were incorporated.

The IRR was digitally signed on July 14, 2000 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.

Origins. The Act traces its roots to the United Nations Commission on International Trade Law ("UNCITRAL") Model Law on Electronic Commerce ("Model Law") and Singapore's Electronic Transactions Act ("ETA"). The Model Law was drafted and adopted by UNCITRAL on December 16, 1996 with the intention of achieving a harmonized legal framework for electronic commerce across multiple borders. The Model Law, as the name implies, was drafted with the intention of being adopted as legislation in various countries around the world. Hence, it was written with a view to maximize acceptability in various legal systems while minimizing any adverse inconsistencies in the international arena. The driving force behind the Model Law was the conviction that a secure legal environment supportive of e-commerce would lead to its promotion and growth.

Singapore's ETA is likewise based upon the Model Law. The ETA was used as a reference for the Act largely because of its provisions on digital signatures, regulation of certification authorities, and service provider liability. However, the provisions on digital signatures and the regulation of certification authorities were abandoned in Congress. This was deemed necessary since the complexity of the underlying issues relating to asymmetric cryptosystems threatened to delay the passage of the Act. It was also recognized that digital signature legislation would be premature since no

certification authority was operating in the country at that time.

The Necessity for the Act. In the months leading to the passage of the Act, members of the legal profession debated the necessity of passing legislation on electronic commerce. On the one hand, there were those who believed that such legislation would be useful to fill in some gaps in Philippine law requiring certain contracts be in "writing" (e.g., the Statute Of Frauds) or that some documents be "signed" (e.g., negotiable instruments). At the other end of the spectrum were those who did not see the necessity for the Act and argued that since the law already recognizes verbal or oral agreements, there should be no reason why electronic contracts should be denied validity.

What could not be denied, however, was the unsettled legal question: do electronic documents and signatures enjoy the same legal status as paper documents and manually signed signatures, respectively? Philippine jurisprudence had not categorically validated electronic evidence. In a recent case, the Supreme Court declared electronic mail inadmissible – but this was due to the fault of the offering party who merely printed out the said messages and failed to have them authenticated or certified as accurate (*IBM Philippines, Inc. v. NLRC*, 305 SCRA 592 [1999]). Under these circumstances, even if the evidence were in the form of paper documents, they would be inadmissible for lack of proper authentication.

To make matters worse, it was universally acknowledged that the settlement of the legal issues respecting electronic contracting and evidence would take years, if not decades, if left in the hands of the Philippine judiciary. Notably, the only source of binding case law in the Philippines are the decisions of the Supreme Court. Meanwhile, absent any existing legal framework for electronic commerce,

the state of law would at best be in a state of flux and may very well be a hindrance to the promotion of electronic commerce in the country.

Hence, the brewing debate among lawyers and judges only highlighted the fact that there was at least a *doubt* respecting the validity of e-commerce transactions. Unfortunately, the absence of a clear consensus among legal experts only created an atmosphere of uncertainty especially among those in the business community. Such uncertainty in turn brought fear which stifled investment and entrepreneurship as businessmen readily dismissed e-commerce as an all-too risky endeavor. The only solution to the conundrum therefore, was to pass the Act and expressly recognize, in no uncertain terms, that doing business electronically is *legal, valid and binding*.

Guiding Principles of the Act. The primary guiding principle behind the Act is the “functional equivalent” approach. In simple terms, the *functions* of say, a document or a signature is analyzed, and if an *equivalent* exists in electronic form, then it will be adopted. For example, a signature performs the function, among others, of identifying the signer and indicating his consent to a document. If an electronic method performs the same functions, then such method would be considered an electronic signature.

Apart from the “functional equivalent” approach, the Act is likewise technology neutral – that is, it does not favor any particular technology. It has long been recognized that if laws are not technology-neutral, they would have an adverse impact against competing technologies. A technology-specific statute would encourage the private sector to support only that technology which consequently establishes it as a single or sole standard. If this persists, it will inevitably result in a dearth of innovation and inventiveness as

all resources will be devoted to sustain the favored technology. To avoid this, the Act was written with an overriding concern to embrace the full range of electronic technology without bias or prejudice. Thus, the Act does not discriminate among any type of electronic document or signature utilizing a particular technology. At most, the Act specifies standards and criteria but the same are written in a neutral manner. For example, the Act admits all types of security measures and the parties are free to determine the type and level of security needed for their transactions and to select and use or implement appropriate technological methods that suit their needs.

A necessary adjunct to technology neutrality is the principle of media neutrality which is likewise ingrained in the Act. In sum, the Act will recognize electronic documents and signatures in whatever media they may be found. For example, if an electronic message is received both as an electronic mail and fax, both of them will be considered an electronic data message or electronic document.

Role of the Act vis-à-vis Philippine Law. The Act is not intended nor designed to supplant any substantive law, particularly on contracts. Activities which were lawful (or unlawful) prior to the passage of the act generally retain their status. This is, of course, excepted by the new crimes which are defined in the Act.

It is important to remember that the Act only affects the *form* of transactions and activities and not their underlying legal validity. In other words, Philippine substantive law will continue to apply

Section 2. Authority of the Department of Trade and Industry and Participating Entities. The Department of Trade and Industry (DTI) shall direct and supervise the promotion and development of electronic commerce in the coun-

try with relevant government agencies, without prejudice to the provisions of Republic Act. 7653 (Charter of Bangko Sentral ng Pilipinas) and Republic Act No. 8791 (General Banking Act).

Authority of DTI to Set Forth Policies. This provision of the Act was placed in this section of the IRR in order to establish the authority of the DTI, DBM and BSP to lay down the policies for the promotion of electronic commerce set forth in Chapter II.

Chapter II - Declaration of Principles for Electronic Commerce Promotion

Section 3. Principles. Pursuant to the mandate under Section 29 of the Act to direct and supervise the promotion and development of electronic commerce in the country, the following principles are hereby adopted as Government policy on electronic commerce:

Source of the Policies. The policies in Chapter II were based on the Global Action Plan for Electronic Commerce published by the Alliance for Global Business (AGB).

a) *Role of the Government.* Government intervention, when required, shall promote a stable legal environment, allow a fair allocation of scarce resources and protect public interest. Such intervention shall be no more than is essential and should be clear, transparent, objective, non-discriminatory, proportional, flexible, and technologically neutral. Mechanisms for private sector input and involvement in policy making shall be promoted and widely used.

b) *Role of the Private Sector.* The development of electronic commerce shall be led primarily by the private sector in response to market forces. Participation in electronic commerce shall be pursued through an open and fair competitive market.

Electronic Commerce will be Private Sector Led. The development of electronic commerce should be driven by market forces with minimal government intervention. Government's role is nonetheless important insofar as it must provide and sustain a secure legal environment and a competitive business environment for electronic commerce.

c) *International Coordination and Harmonization.* Electronic commerce is global by nature. Government policies that affect electronic commerce will be internationally coordinated and compatible and will facilitate interoperability within an international, voluntary and consensus-based environment for standards setting.

Harmonization of Laws. Electronic commerce, especially those conducted over the Internet, are necessarily global in nature. This means the companies engaged in electronic commerce will be required to comply with the laws of each country where they can potentially close transactions.

On the one hand, inconsistent laws in varying jurisdictions can be exploited by any e-commerce company. Hence, countries with lax rules or enforcement may find themselves used as a "safe harbor" for e-businesses performing acts or rendering services otherwise illegal or immoral in their home countries. For example, a New York-based on-line gambling website operates out of a casino in Antigua where the servers are located – this despite the fact that gambling is illegal in New York.

On the other, dissimilar laws can also pose problems for the e-commerce venture. Take the case of a certificate authority which must comply with varying accreditation rules in different countries. In some cases, the failure to comply may expose them to criminal liability. Hence, burdensome laws in some coun-

tries may become a deterrent against electronic commerce companies wishing to operate on a global basis.

In this regard, it is desirable to have laws on electronic commerce which are consistent throughout the world in order to promote the growth of these "global" e-businesses.

Jurisdiction. Initially, SB 1523 and HB 9971 contained the following provision on jurisdiction:

Section 26. *Jurisdiction* - An electronic contract dealing with the use of a key management system shall indicate the jurisdiction whose laws apply to that system or whose law shall apply to the contract. In the absence of such indication, jurisdiction over the contract shall be acquired in accordance with existing laws (HB 9971).

During the interpellation period at the Senate, Sen. Juan Ponce Enrile raised the question as to what existing law determined the jurisdiction of electronic commerce transactions. He gave the example of a Filipino surfer who purchases an item from Amazon.com and asked where the sale consummated. In addition, which law (US or Philippine) would apply to the transaction in case of a dispute.

In recognition of the complex and unresolved issues concerning jurisdiction over electronic and Internet commerce transactions, the Bicameral Conference Committee decided to drop this provision from the Act.

d) *Neutral Tax Treatment.* Transactions conducted using electronic commerce should receive neutral tax treatment in comparison to transactions using non-electronic means and taxation of electronic commerce shall be administered in the least burdensome manner.

Taxation in the Bills. SB 1902 contained the following provision:

SEC. 27. *Taxes on E-Commerce Transactions.* - Value-

added, sales and other appropriate taxes shall be collected on E-commerce transactions by the central and local governments concerned.

It was determined, however, that since tax laws do apply with equal force upon electronic transactions, the above-quoted provision was unnecessary and was therefore abandoned during the Bicameral Conference Committee meeting.

Taxation of Electronic Commerce. There are to date, no explicit Philippine tax laws on electronic commerce and it appears that no law will be passed on this subject matter in the near future. However, it is undeniable that many of the activities involving electronic commerce are subject to existing tax laws. For example, the retail of goods over the Net would attract value-added taxes (VAT). Additionally, all electronic commerce entities located in the Philippines would be subject to some form of income taxation, indirect taxes, and even local government taxation. The goal of the policy is to encourage the taxing authorities to treat electronic commerce entities no different from the bricks-and-mortar counterparts. Again, this is viewed as promoting the growth of electronic commerce.

e) *Protection of Users.* The protection of users, in particular with regard to privacy, confidentiality, anonymity and content control shall be pursued through policies driven by choice, individual empowerment, and industry-led solutions. It shall be in accordance with applicable laws. Subject to such laws, business should make available to consumers and, where appropriate, business users, the means to exercise choice with respect to privacy, confidentiality, content control and, under appropriate circumstances, anonymity.

Internet Consumer Trust Issues. When the Internet was developed, the academics designing the same were not particularly concerned about ano-

nymity (because everyone knew each other) and confidentiality (because they all trusted each other). Neither did they envision the Net to become universally accessed by millions of users. They instead focused their efforts on making the Internet the efficient, robust and reliable network we find today. The end result is an Internet where electronic mail enjoys the same privacy as postcards and users can easily mask their identity or even assume the identity of another. In addition, emerging technologies empowered users to collect vast amounts of personal information which, in electronic form, can more easily be sold or disclosed to third parties. This is a classic case where the technology outpaced the law leaving fertile ground for unscrupulous persons to abuse the vacuum. Hence, the policy espouses market-led solutions to these controversial Internet issues. This is deemed to be necessary given that neither the passage of laws nor the adjudication of disputes by courts would be adequate either to solve existing problems or to keep pace with the rapidly changing environment.

f) *Electronic Commerce Awareness.* Government and the private sector will inform society, both individual consumers and businesses, about the potentials of electronic commerce and its impact on social and economic structures.

g) *Small and Medium-Sized Enterprises.* Government will provide small and medium-sized enterprises (SMEs) with information and education relevant to opportunities provided by global electronic commerce. Government will create an environment that is conducive to private sector investment in information technologies and encourage capital access for SMEs.

h) *Skills Development.* Government shall enable workers to share in the new and different employment generated by electronic commerce. In this regard, the Government shall continue to promote both formal and non-formal skills-

development programs.

i) *Government as A Model User.* Government shall utilize new electronic means to deliver core public services in order to demonstrate the benefits derived therefrom and to promote the use of such means. In this regard, the Government will be a pioneer in using new technologies. In particular, the Government Information System Plan (GISP), which is expected to include, but not be limited to, online public information and cultural resources, databases for health services, web sites at local, regional and national levels and public libraries and databases, where appropriate, will be implemented in accordance with the provisions of the Act and RPWEB.

j) *Convergence.* Convergence of technologies is crucial to electronic commerce and will be supported by appropriate government policies. Government will work closely with business in preparing for and reacting to changes caused by convergence.

k) *Domain Name System.* The Government supports initiatives to ensure that Internet users will have a sufficient voice in the governance of the domain name system.

l) *Access to Public Records.* Government shall provide equal and transparent access to public domain information.

m) *Dispute Mechanisms.* Government encourages the use of self-regulatory extra-judicial dispute settlement mechanisms such as arbitration and mediation as an effective way of resolving electronic commerce disputes. (n)

Alternative Modes of Dispute Resolution. While the Philippine Judicial Academy is in the process of educating members of the judiciary on Internet and electronic commerce legal issues, the pace of technology will outstrip the ability of courts to become an effective venue for the resolution of electronic commerce disputes. Hence, electronic commerce players would be better served by privately-run dispute resolution centers with

the expertise and infrastructure to handle complex disputes in a virtual environment. Such centers would have arbiters with the necessary technical and legal expertise to dispense justice in an even-handed manner.

This vision has to date become a reality. Initiatives by the Internet Corporation on Assigned Names and Numbers (ICANN) have established an arbitration process for handling domain name cybersquatting cases which has so far been successful at curbing this insidious practice. For more information, visit www.icann.org.

Chapter III - Objective and Sphere of Application

Section 4. *Objective of the Act.* The Act aims to facilitate domestic and international dealings, transactions, arrangements, agreements, contracts and exchanges 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.

Objective. The primary objective of the Act is to provide a secure legal framework and environment for electronic commerce. This is pursuant to the notion that such an environment will promote electronic commerce. In the case of the Philippines, this has come to pass as investments into electronic commerce ventures have been steadily rising following the passage of the Act.

Section 5. *Sphere of Application.* The Act shall apply to any kind of electronic data message and electronic document used in the context of commercial and non-commercial activities to include domestic and international deal-

ings, transactions, arrangements, agreements, contracts and exchanges and storage of information.

Unique Feature of the Act. Unlike similar legislation in other countries, the Act applies equally to commercial and non-commercial activities. Note that the Model Law was intended to govern electronic commercial transactions only. Hence, the bills considered by both houses of Congress were likewise limited and excluded non-commercial transactions. However, during the House deliberations, the authors and co-lead sponsor of the bill, Rep. Leandro Verceles (Lone District, Catanduanes), shared the view that the law should have universal application. Hence, amendments were introduced to expand the scope of the Act to cover non-commercial transactions.

The principal reason behind the expanded coverage was simple: unlike the Model Law, the Act deals with decidedly "non-commercial" electronic activities such as the performance of government functions and the definition of hacking as a criminal offense. Furthermore, there seemed to be no reason why non-commercial events and transactions should be excluded from the law's application when a substantial portion of the Internet traffic in the Philippines was not business-related. Finally, it was also believed that a limited application of the Act would create confusion and unintended consequences. For example, a person accused of hacking a charitable site for fun could argue that since the act was not done for commercial purposes, none of the electronic evidence would be admissible. If upheld, that would, of course, allow him to evade prosecution.

The question would then arise as to what transactions are commercial and what are not. The distinction would be of utmost importance because the latter could neither be under-

taken electronically nor proven using electronic evidence. This creates a double standard that fosters even more confusion. For instance, a person accused of sending threatening e-mails (e.g., "I'm going to kill your dog!") might argue that since the communication was personal and not commercial, the e-mails are inadmissible and invalid under the Act. But if the threats were directed at the commercial interests of the victim (i.e., "I'm going to burn down your store!"), the Act may be said to apply.

At any rate, the foregoing illustrates that a limited application of the Act to commercial transactions only gives rise to more legal problems.

In other situations, such a limited application can cause injustice. An illegitimate child for example would not be permitted to submit an admission of filiation by his putative father if the same were contained in an e-mail message. In such decidedly non-commercial activities, the electronic evidence would be useless to the party-litigant.

Finally, a limited application would make the Act static and inflexible to adapt to the rapid pace of technology. It is undeniable that new technologies will introduce changes in *all* aspects of modern living. Already there are web-enabled refrigerators that keep track of their contents; automatically suggest what dishes to cook; and place online orders to the store for groceries. Inevitably, electronic documents and signatures will find widespread application, commercial as well as non-commercial. It is, therefore, with a measure of foresight that the Philippine Congress decided to adopt a universal application for the Act.

Non-Commercial Applications. By expanding the scope of the Act, electronic documents and signatures may now be used in all types of transactions and acts. More importantly, electronic evidence is now admissible in all types of civil, criminal and administrative actions.

Non-commercial activities include, among others, acts, transactions and documents relating to national security, criminal offenses, marriage, paternity and filiation, adoption, parental authority, donations, quasi-delicts, labor and employment, labor relations, elections, suffrage, agrarian reform, immigration, and protection of the environment.

PART II

ELECTRONIC COMMERCE IN GENERAL

Chapter I - General Provisions

Section 6. *Definition of Terms.* For the purposes of the Act and these Rules, the following terms are defined, as follows:

(a) "Addressee" refers to a person who is intended by the originator to receive the electronic data message or electronic document, but does not include a person acting as an intermediary with respect to that electronic data message or electronic document.

Who is an Addressee. Under Philippine law, natural and juridical persons have the capacity to act with legal consequences. They are therefore the subject of laws and are the parties to contracts and transactions. Hence, under the Act an "addressee" must always be a natural or juridical person.

In addition, intent plays a role in determining the addressee of electronic data messages. Hence all persons who might chance upon the data message or play a role in its transmission are excluded from the term addressee. This also takes into consideration the possibility that data messages are handled by assistants or employees of the intended addressee who oftentimes have direct access to say, the addressee's electronic mailbox.

Consistent with the Model Law, the Act should not be misinterpreted as allowing for a computer to be made the subject of rights and obligations (§35, UNCITRAL Model Law on Electronic Commerce with Guide to Enactment; the "Guide"). For example, computers which are programmed to automatically match buy and sell orders are not the parties to the transaction. In such cases, the parties are the persons in whose behalf the data messages (*i.e.*, the electronic buy and sell orders) were sent. This emphasizes that networks and computers are merely conduits or tools by which transactions are facilitated. A computer is no less a party to a contract as a fax machine or other office tool.

Note that the terms "person" and "intermediary" which are used in this Section are separately defined in the IRR.

(b) "Commercial Activities" shall be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. The term shall likewise refer to acts, events, transactions, or dealings occurring between or among parties including, but not limited to, factoring, investments, leasing, consulting, insurance, and all other services, as well as the manufacture, processing, purchase, sale, supply, distribution or transacting in any manner, of tangible and intangible property of all kinds such as commodities, goods, merchandise, financial and banking products, patents, participations, shares of stock, software, books, works of art and other intellectual property.

Origin of Provision. This provision is lifted from a footnote appearing in the Guide. Note that the definition of "non-commercial activities" is merely those which are excluded from the above-definition.

(c) "Computer" refers to any device or apparatus singly or in-

terconnected which, by electronic, electro-mechanical, optical and/or magnetic impulse, or other means with the same function, can receive, record, transmit, store, process, correlate, analyze, project, retrieve and/or produce information, data, text, graphics, figures, voice, video, symbols or other modes of expression or perform any one or more of these functions.

What is a Computer. Note that the above definition is merely an elaboration of the term "Information and Communications System" which includes computers. The definition is likewise broad enough to include all types of electronic equipment including desktop and mobile computers, fax machines, scanners, printers, computer monitors, card readers, smart cards, credit cards, ATM cards, mobile phones, pagers, radios, VCRs, video equipment, audio equipment, personal digital assistants ("PDAs"), answering machines and telephones. In the near future, even ordinary household appliances such as the refrigerator and washing machine may be deemed computers as devices allowing them to communicate over the Internet, among others, are developed.

(d) "Convergence" refers to technologies moving together towards a common point and elimination of differences between the provisioning of video, voice and data, using digital and other emerging technologies; the coming together of two or more disparate disciplines or technologies; the ability of different network platforms to carry any kind of service; and the coming together of consumer devices such as, but not limited to, the telephone, television and personal computer.

Origin of the Definition. The definition of convergence was deemed necessary because of Section 28 of the Act relating to RPWEB. The above-definition was based primarily upon Sen-

ate Bill No. 1556 otherwise known as the Convergence Bill.

(e) "Electronic data message" refers 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. Throughout these Rules, the term "electronic data message" shall be equivalent to and be used interchangeably with "electronic document."

Origin. The definition of "electronic data message" was based on the Model Law's definition of "data message". The Act however deleted the final phrase which enumerated examples but this was restored in the IRR.

Interchangeability with "Electronic Document." The final sentence relating to the term's interchangeability with "electronic document" was called for because the technical working group of the Bicameral Conference Committee intended the terms to be equivalent. Note that the Senate version of the Act defined the term "electronic data message" while the House version of the Act adopted the term "electronic document." In order to simplify the merging of the both versions, both terms were adopted.

It is submitted, however, that the term "electronic data message" is broader in scope than "electronic document." The interchangeability of the terms therefore allowed the Act to embrace a wider set of electronic documents.

Electronic Data Message. An electronic data message is composed of its contents – the Act uses the word "information." This is consistent with the functional equivalent approach because in the real world, documents are relevant only in terms of the information held within their four corners. In fact, the Rules of Evidence state that documents are "offered as proof of their contents" (Sec. 2, Rule 130, Rules

of Court). It is clear, therefore, that the paper or medium containing the information is irrelevant even in real world documents. In rare instances where they are relevant – such as those involving treasury certificates, land titles and legal tender, the paper itself is considered object evidence, not documents.

Generally, the term “electronic data messages” should be understood to mean any electronic file. What differentiates an electronic data message from its real world counterpart, however, is the manner in which the underlying information is handled. The Act provides that such information is “generated, sent, received or stored by electronic, optical or similar means.” These terms may be best understood by giving the following examples:

- “*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. Such electronic files therefore enjoy the same protection under the Act.

This likewise refers to situations where paper documents are transformed into paperless form by digital imaging or scan-

ning. What was once a paper document is now 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.

As an analogy, think of the electronic data message as wine contained in a bottle. The wine may be poured into a glass or a flask but all times, it retains its character as wine separate and distinct from its containers. One should never confuse the wine with the bottle. Hence, one should not think of an electronic document merely as a computer file but the information contained therein. Even if it is printed out on paper, it retains its character as an electronic data message so long as the information has not been altered.

Similar Means. The use of the words “electronic, optical or similar means” is intended to reflect the fact that like the Model Law, the Act was intended to cover not only existing communications systems but technological developments which could not reasonably be foreseen at this time (§31, Guide).

(f) “Information and Communications System” refers to a system for 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.

Origin. This term is based on

the definition of “information system” in the Model Law. The defined term “computers” is subsumed under “information and communications systems.”

Scope. The definition is intended to cover the entire range of technical means used for transmitting, receiving and storing information (§40, Guide). It includes local area networks, wide area networks, the Internet, as well as wireless networks such as GSM.

(g) “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.

Origin. The above-definition was based on Section 2 of the ETA. The Model Law did not have a separate defined term for electronic signature because under that framework, an electronic signature is merely a form of data message – one that performs the function of a real world signature.

Electronic Signatures. Contrary to popular belief, an electronic signature is not necessarily a digitized image of a handwritten signature – although it would qualify as an electronic signature. To better understand the definition, one must apply the functional equivalent approach to electronic signatures.

A signature is used, among others, to identify a person. Applying the functional equivalent approach, anything in electronic form which identifies a user can be said to be his signature if it is logically attached to an electronic data message. For example, if Bill Gates identifies himself in his e-mail messages as follows: “bill gates”, then the

latter would be considered an electronic signature. Alternatively, he could file attach a digital image of his handwritten signature to an encrypted data message and it, too, may be considered as an electronic signature. Yet another example of an electronic signature is the name of a person appearing in the "From" field on an e-mail. Because it identifies a particular person and is logically affixed on an electronic data message, it may qualify as a signature.

A signature can also be used to indicate a person's consent to the contents of or to authenticate a document. In these situations, the electronic signature will not simply be the distinctive mark but will include other information contained in the electronic document. For example, if Bill Gates wanted to approve an e-mail proposal, he might write a reply e-mail with nothing but the word "accepted" plus the usual mark "bill gates". The entire reply e-mail would then constitute the electronic signature.

Another form of electronic signature under the definition is a method employed by the signer to authenticate a data message. This refers to a digital signature but it also contemplates a situation where a person signifies his consent to an online contract by filling up a registration form and clicking on the "I Accept" button. In such cases, the entire methodology (*i.e.*, the contents of the form plus the fact of clicking) will be considered as the electronic signature of the person. This is true also in the case of digital signatures where the signature is not merely the person's public key or his digital certificate but the entire authentication method utilized.

Definition can be misleading. Note that while electronic signatures are defined in the Act, only those which comply with the stringent requirements of Section 8 of the Act or Section 13 of the IRR, rise to the level of and are given the same legal protection as handwritten signatures.

This is an important point which has consequences which will be discussed below in relation to Section 13 of the IRR.

(h) "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. Throughout these Rules, the term "electronic document" shall be equivalent to and be used interchangeably with "electronic data message."

(i) "Electronic key" refers to a secret code, which secures and defends sensitive information that crosses over public channels into a form decipherable only by itself or with a matching electronic key. This term shall include, but not be limited to, keys produced by single key cryptosystems, public key cryptosystems or any other similar method or process, which may hereafter, be developed.

Relevance of Definition. The above-definition is relevant only in the context of lawful access and the obligation to maintain confidentiality referred to in Sections 31 and 32 of the Act or 46 and 47 of the IRR. Note that the definition of this term in the Act (Sec. 5[g]) states that the key is "decipherable only with a matching key." This implied that only electronic keys used within the context of a public key cryptosystems were included. Therefore, the definition in the IRR was expanded to include keys used in single key or symmetric cryptography.

(j) "Intermediary" refers to a person who in behalf of another person and with respect to a particular electronic data message or electronic document sends, receives and/or stores or provides other services in respect of that

electronic data message or electronic document.

Source. This was based upon the same defined term in the Model Law.

Intermediary. Note that the intermediary is excluded from the definition of addressee and originator precisely because the Act intends that only the latter are the parties to electronic transactions. Still, the role of intermediaries in electronic communications is undeniably important. Such intermediaries may be Internet Service Providers, telephone companies, or value-added network services providers. Note also that the definition relates to a particular electronic data message thus recognizing that the same person could be the originator or addressee of one electronic data message but an intermediary with respect to another (§139, Guide).

(k) "Non-Commercial Activities" are those not falling under commercial activities.

(l) "Originator" refers to a person by whom, or on whose behalf, the electronic data message or 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 data message or electronic document.

Originator. During the Senate interpellation on SB 1523 (later SB 1902), Sen. Defensor-Santiago set forth a scenario where a computer is programmed to accept electronic offers automatically. She asked, is the computer the party to the contract? Under this provision, the party to the agreement is the person in whose behalf the electronic acceptance was sent. Note that as with the Model Law, the originator and the addressee are "persons", *i.e.*, natural persons or juridical entities.

Note also that an originator also includes one who creates

an electronic document not for transmission but only for storage (§37, Guide).

(m) “Person” means any natural or juridical person including, but not limited to, an individual, corporation, partnership, joint venture, unincorporated association, trust or other juridical entity, or any governmental authority.

(n) “Service provider” refers to a provider of -

i. Online services or network access, or the operator of facilities therefore, including entities offering the transmission, routing, or providing of connections for online communications, digital or otherwise, between or among points specified by a user, of electronic data message or electronic documents of the user’s choosing; or

ii. The necessary technical means by which electronic data message or electronic documents of an originator may be stored and made accessible to a designated or undesignated third party.

Such service providers shall have no authority to modify or alter the content of the electronic data message or electronic document received or to make any entry therein on behalf of the originator, addressee or any third party unless specifically authorized to do so, and shall retain the electronic data message or electronic document in accordance with the specific request or as necessary for the purpose of performing the services it was engaged to perform.

Service Provider. This definition is relevant in relation to Section 30 of the Act on the liability of service providers. It is immediately clear that VANs and ISPs are included in the term service provider. However, it also includes application service providers, web hosting companies, domain name registries and registrars, online exchanges, websites hosting discussion groups and perhaps, any conceivable web-based online service company. In the case of SMS texting or even voice messaging, a cellphone

company may be considered a service provider. The same is true for telephone companies in relation to their transmission of electronic data messages such as faxes or voice messages.

Chapter II - Legal Recognition of Electronic Data Messages and Electronic Documents

Section 7. *Legal Recognition of Electronic Data Messages and Electronic Documents.* 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:

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.

Source. Section 6 of the Act merges Articles 5 and 5bis of the Model Law.

Fundamental to the Act. This provision embodies the fundamental principle that electronic documents should not be discriminated against but should be given the same legal status as their paper-based counterparts. Note that the first sentence states the rule in the negative to emphasize that the law validates or confirms the legality of the form of the electronic document, not its contents *per se*. In other words, the law does not automatically state that the information in the electronic document is legal or valid – it might very well be criminal. But such information shall not be denied recognition or effect solely because it is contained in an electronic document.

Sub-paragraphs (a) to (d) merely elaborate upon the rule enunciated in the provision. Subparagraph (d) applies to requirements under different laws for the posting of notices (such as in extra-judicial foreclosures) or the delivery of documents (such as the service of summons).

The entire Section should be read in conjunction with Section 10 of the IRR which specifies additional requirements before the electronic document can be considered a “writing” under Philippine law.

Section 8. *Incorporation by Reference.* Information shall not be denied validity or enforceability solely on the ground that it is not contained in an electronic data message or electronic document but is merely incorporated by reference therein.

Relevance of this Provision. This Section was separated from the latter portion of Section 6 of the Act to emphasize the importance of the provision as well as to harmonize the structure with the Model Law. It is expected that many of the electronic documents and data messages that will be used in electronic commerce will no longer contain all relevant information but mere

references thereto. For example, a standard e-mail contract might have a hyperlink to the standard terms and conditions applicable to the agreement instead of a full recital in the same message. This practice not only simplifies transactions but also saves systems and network resources. Additionally, much of electronic commerce occurs through coded messages that are intelligible when related to information outside the said message. Under this provision, the coded message may be considered a contract or a valid document.

Section 9. Use Not Mandatory. Without prejudice to the application of Section 27 of the Act and Section 37 of these Rules, nothing in the Act or these Rules requires a person to use or accept information contained in electronic data messages, electronic documents, or electronic signatures, but a person's consent to do so may be inferred from the person's conduct.

Freedom to Opt Out. The principle embodied in this provision is implied in Section 16(1) of the Act (Section 21 of the IRR) where it provides (in the opening phrase thereof) that parties are free to provide that their contract or agreement will not be in electronic form. Despite such implicit recognition, the above provision was included in the IRR to assuage concerns among those not ready nor willing to engage in electronic commerce. Hence, if a person receives an e-mail offer to enter into an electronic contract, such person is free to ignore the same and request the counter-party to conduct the transaction off-line. In fact, many on-line retailers advertise their toll-free numbers as an alternative method of conducting business with their customers.

The reverse of the rule is likewise true in that parties may not compel others to conduct business in a paper-based environment. Hence, a purchaser of an

on-line retailer would not have the option to force the e-tailer to a paper-based transaction against the latter's will.

Exception. As an exception to this rule, however, the conduct of a person may be used as evidence of his consent to enter into an electronic contract. For example, if a person purchases a book through an on-line retailer, the purchaser will not be heard to deny the validity of the electronic transaction. It is obvious that his consent to the electronic transaction can be inferred from his conduct.

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.

Classes of Electronic Documents in the Model Law. Under the Model Law, there are two (2) major classes of electronic documents – “writings” and “originals.” All electronic data messages are considered “writings” so long as they are “accessible so as to be usable for subsequent reference” (Article 6, Model Law). In other words, for “writings” the Model Law only focused upon the basic notion of the information being reproduced and read (§49, Guide). Apart from the foregoing, “writings” were not

required to conform to any other requirement such as that relating to unalterability or reliability. This is consistent with the idea that since not all paper-based documents are free from unauthorized alteration and forgery, the same should not be imposed upon electronic documents. Hence, forged or fraudulent electronic documents should enjoy the evidentiary benefits of admissibility and legal effect as their paper-based counterparts.

From another perspective, it may be said that the integrity and reliability of electronic “writings” should be presumed as with paper documents. Any doubt relating to their authenticity should be established by clear and convincing evidence and not upon the mere allegation or speculation by the party against whom such electronic document is presented.

Hence, under the Model Law where the law provides that certain information must be “in writing” or be embodied in a “written document” (e.g., the Statute of Frauds), an electronic “writing” will suffice.

A “writing” however is to be distinguished from an “original.” “Original” electronic documents are important in the context of say, bills of lading, certificates of deposits and negotiable instruments in which the notion of uniqueness of an original is particularly relevant (§63, Guide). For example, the original of a negotiable bill of exchange must be presented to the drawee for acceptance. In the context of an electronic bill, a higher degree of authenticity is required in order to preserve faith in these instruments. Applying the functional equivalent approach, the Model Law requires electronic “originals” to possess “a reliable assurance as to the integrity of the information” (Article 8[1][a], Model Law) and the ability to be displayed to the person to whom it is to be presented (Article 8[1][b], Model Law).

Evidently, reliability and integrity are essential to “originals”

while, in contrast, these attributes are dispensable for “writings.” In the hierarchy of documents under the Model Law, therefore, “writings” possess a lower degree of authenticity and genuineness than “originals.” This is permissible because of the peculiar demands made upon “original” electronic documents.

Classes of Electronic Documents in the Act. The hierarchy of documents under the Model Law finds ready application under Philippine law. However, the Act did away with the clear distinction between “writings” and “originals.” Note that under Section 10 of the IRR, “writings” must maintain their integrity and reliability. Under Section 11 of the IRR, the same requirements must be met.

The effect of the blurring of this distinction is that where Philippine law requires something to be in “writing,” the electronic data message or electronic document must have some measure of integrity and reliability. Otherwise, it will not be considered a “writing.” In practical terms, if an electronic document fails to meet the standards under Section 10 above, it cannot be used to satisfy the requirements of say, the Statute of Frauds which requires the sale of goods valued at more than five hundred pesos (P500.00) to be in writing. From the standpoint of a party-litigant who wishes to impugn that electronic document of sale, the latter can now raise issues of integrity and reliability in order to deny the electronic document the status of a written document. This is a unique defense which would not otherwise have been available if the Act had adopted the less stringent rule in the Model Law that electronic data messages are “writings.”

That is not to say, however, that the electronic document is entirely useless – its contents (*i.e.*, information) has legal effect and may still be referred to and presented as evidence in court. However, because it fails to pos-

sess the integrity and reliability required of “writings,” the electronic document will not rise to the same status as a written document.

The more stringent requirements of Section 10 vis-à-vis electronic “writings” will have an adverse impact upon the following documents which are required to be in “writing”:

(a) Those falling under the Statute of Frauds (Art. 1403[2], Civil Code);

(b) Negotiable instruments (Sec. 1, Negotiable Instruments Law);

(c) Donations of personal property with value in excess of 5,000 pesos (Art. 748, Civil Code);

(d) Contract of antichresis where the amount of the principal and interest must be in writing (Art. 2134, Civil Code);

(e) Stipulation to pay interest on loans (Art. 1956, Civil Code);

(f) Power of attorney to sell land or any interest therein (Art. 1874, Civil Code);

(g) Assignment of copyright in whole or in part during the lifetime of the author (Section 180.2, Intellectual Property Code);

(h) Marriage Settlements (Art. 77, Family Code); and,

(i) Stipulations limiting a common carrier’s liability to less than extraordinary diligence (Art. 1744, Civil Code)

The blurred of the distinction between electronic “writings” and “originals” likewise had the effect of creating another class of electronic documents under the Act. These are electronic documents which are not required by law to be “in writing” for their validity and likewise free from the constraints of being presented or displayed in their “original” form. Instead, they are merely evidence of the information contained therein – nothing more.

An example would be an e-mail which contains an admission of a particular fact say, of the writer’s negligence during a

recent mishap. The electronic document is not a “writing” because it is not required by law to be in written form. There is likewise no legal necessity to keep the same in some “original” form. But the Act nonetheless gives legal significance to the e-mail’s contents and authorizes its admission into evidence. It is submitted that a large number of electronic documents will fall under this category.

Integrity. Under Section 10 of the IRR, an electronic “writing” must maintain its integrity. This is established by showing that “(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” (Section 10[b][i], IRR). Hence, the addition of message headers, digital signatures, and other marks to the electronic document will not detract from its status as a “writing.” Real world counterparts would be “received” or “sent” stamps which are affixed on paper documents in the course of delivery.

Reliability. Note that the standard of reliability is determined by the surrounding circumstances. In other words, each situation must be examined to determine the reliability of electronic documents. If a person usually employs encryption to all his e-mails, an unencrypted e-mail which purports to originate from him may be considered unreliable whereas, the plain e-mail may be considered reliable vis-à-vis ordinary users. It will be observed that the reliability analysis is subjective in nature and reliance upon circumstances which are deemed relevant may change from person to person.

Section 11. Original. 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.

What are "Originals." "Original" electronic documents are legally relevant and significant only if they retain their uniqueness. The real word equivalents of "original" electronic documents are, among others, negotiable instruments (bills of exchange and promissory notes), negotiable instruments of title, stock certificates, deposit certificates, and treasury instruments. With these, 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 faith in and commercial reliance upon such documents in electronic form

might be eroded. For example, an electronic negotiable instrument would lose its status as an "original" if there existed no reliable assurance of its integrity.

Integrity. The standard for integrity for "original" electronic documents differ slightly from electronic "writings." For "originals", the integrity must be shown to exist "from the time when it was first generated in its final form." This is intended to include the situation where the document was first composed on paper and later transferred to the computer. In such a situation, the Act is to be interpreted as requiring assurances that the information remained complete and unaltered from the time it was composed as a paper document onwards, and not merely from the time it was translated into electronic form (§66, Guide).

Originals and the Best Evidence Rule. The Best Evidence Rule states that when a document is the subject of inquiry, no evidence shall be admissible other than the original document itself (Section 3, Rule 130, Rules of Court). If taken in the context of the Act, it would appear that all electronic documents to be presented in evidence must comply with the requisites of an "original" (*i.e.*, maintain their integrity and reliability under Section 11, IRR).

The final paragraph of the above section however, implies that this is not the case. It states that with respect to electronic data messages and electronic documents, the mere fact that they comply with Sections 6 and 7 of the Act will render them the best evidence of the agreement or transaction contained therein. This means that electronic data messages *by themselves* are considered an original document for purposes of complying with the Best Evidence Rule. In this regard, the electronic document need not comply with the requirements of Section 11 of the IRR relating to "originals"— that is, the party presenting the electronic document as an original

under Best Evidence Rule is not required to prove either its integrity or reliability.

However, the above conclusion should be interpreted within the context of Sections 6 and 7 of the Act. 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.

Note finally, that the last paragraph of Section 11 only deals with the Best Evidence Rule and not upon the admissibility of electronic documents in general – a matter which is discussed in Section 18 of the IRR (*supra*). Briefly, an electronic document is considered the functional equivalent of a written document. Hence, the electronic document will have to comply with the same rules governing the admissibility of written documents.

Section 12. Solemn Contracts. No provision of the Act shall apply to vary any and all requirements of existing laws and relevant judicial pronouncements respecting formalities required in the execution of documents for their validity. Hence, when the law requires that a contract be in some form in order that it may be valid or enforceable, or that a contract is proved in a certain way, that requirement is absolute and indispensable.

What are Solemn Contracts. Solemn contracts are those which are valid only if the form prescribed by law is observed. For example, the agreements under the Statute of Frauds must be in writing or they will be unenforceable. However, the provision applies not only to con-

tracts or agreements but documents of all kinds which must be in writing to be valid.

Notarized Documents. In some instances, the law requires that documents be acknowledged before a notary public before they are considered valid. An example is a notarial will which must not only be in writing but must also be signed by at least three (3) witnesses and acknowledged before a notary public. Otherwise, it is invalid and the decedent is deemed to have died intestate.

Under Philippine law, notarized documents enjoy a higher degree of acceptability largely because the Rules of Court considers them public documents which are easier to present in evidence (Section 19[b], Rule 132, Rules of Court). In fact, notarized documents may be presented into evidence without further proof because the notarial acknowledgement is *prima facie* evidence of the execution of the document (Section 30 Rule 132, Rules of Court).

This is distinguished from the treatment of private documents which are admissible only after their authenticity and due execution are established (Section 20, Rule 132, Rules of Court). As a result, many transactions are evidenced by notarized agreements so much so that in the minds of many, a contract is invalid until notarized. This is, of course, largely untrue.

Given this widespread use of notarized documents, the Act provides that the Supreme Court may adopt authentication procedures including electronic notarization systems (Section 11, Act). Originally, the Act was supposed to include provisions regulating electronic notarization and the licensing of "cybernotaries." However, it was feared that the ensuing debate on the issue might delay the passage and approval of the act. Hence, the responsibility was passed on to the Supreme Court. It is hoped that the High Court will issue its regulations

soon since the ability to have electronic notarization will go a long way in promoting the use of electronic means for conducting business.

Legal Recognition of Electronic Signatures

Section 13. *Legal Recognition of Electronic Signatures.* 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.

For purposes of subparagraphs (i) and (ii) of paragraph (b), the factors referred to in Annex "2" may be taken into account.

Rationale. The Senate technical working group crafted this

provision using the ETA as a starting point. Concerns were raised regarding the ease by which electronic signatures may be forged or falsified. Hence, it was deemed necessary to require integrity and reliability from electronic signatures. Furthermore, the ability to independently verify electronic signatures gives comfort to those who may be required to rely upon them. Independent verification was also intended to encourage individuals to conduct their own due diligence respecting the identity of the signer and authenticity of the signature.

The Recognition of Electronic Signatures under the Model Law and the ETA. The Model Law adopted all types and kinds of electronic signatures provided the latter constituted the functional equivalent of manually signed signatures. Hence, Article 7 of the Model Law merely requires that the electronic signature utilize a method to identify a person and to indicate that person's approval of the information contained in the electronic data message. The same wholesale validation of electronic signatures also appears in Section 8 of the Singapore ETA.

This approach is consistent with the aim of the Model Law to be technology-neutral. It likewise embodies the application of the functional equivalent approach. Hence, there exists no discrimination as to any type of electronic signature.

The Limited Recognition of Electronic Signatures under the Act. The Act, however, does not embrace all types of electronic signatures adopted under the Model Law. In fact, the Act imposes strict requirements before an electronic signature qualifies as a handwritten signature. These are set forth in paragraphs (i) to (iv) above and in Section 8 (a) to (d) of the Act.

It is submitted that these requirements were put in place in an attempt to ensure that only reliable electronic signatures are recognized under Philippine law.

Obviously, this was borne out by the lack of trust in electronic signatures in general. This lack of trust can be traced to the ease by which an electronic signature may be forged or falsified. For example, the Act defines a voice print attached to an electronic data message as an electronic signature. However, anyone – even an inexperienced computer user – can merely file attach the same file to another electronic data message and give the latter the appearance of having been “signed” by the owner of the voice print. Hence, in the effort to ensure that only reliable electronic signatures are recognized under the Act, Congress abandoned the functional equivalent approach.

The functional equivalent approach dictates that all electronic signatures should have been made to enjoy the benefits of handwritten signatures. In other words, electronic signatures should enjoy the presumption of validity until this is overcome by contrary evidence. There should likewise be no obstacle to their admissibility in evidence and should be relied in the absence of contrary proof. More importantly, the presumption favoring the reliability, integrity and authenticity of electronic signatures should be overcome by clear and convincing evidence. The party assailing the electronic signature should not be permitted merely to raise doubts or speculate upon the ease of electronic forgery, it should be firmly and clearly established if such is the case.

Sad to say, this was not the approach taken by Congress and as a result, *all* of the electronic signatures commonly used at this time *do not* enjoy the legal status of a handwritten signature. In other words, the average or common e-mail signatures, digitized images of signatures, voice prints, distinctive marks and others are not by themselves considered valid signatures under the Act.

It is submitted however that

the fear surrounding the reliability and integrity of electronic signatures should not have prevented the application of the functional equivalent approach in the Philippines. Congress should have realized that even real world signatures can be forged. In fact, these “real world” forgeries enjoy the presumption of validity until proven otherwise. They may even be admitted into evidence and become the basis of court decisions. Electronic signatures should have enjoyed the same treatment – the presumption of validity until the presentation of clear and convincing evidence to the contrary. Instead, Congress introduced prerequisites before validating an electronic signature under the Act which in effect, discriminates against electronic signatures vis-à-vis handwritten signatures.

What are Valid Electronic Signatures under the Act. It appears that given the requirements relating to electronic signatures, the Act validates *only* digital signatures which exist within the context of public key infrastructure (PKI). Evidently, only these signatures are given the same legal status as handwritten signatures. While there may be other types of electronic signatures in existence or may hereafter be developed which likewise comply with the Act, it is submitted that these are not in widespread use and are therefore largely irrelevant to the Act.

Effect of Limited Recognition. It is the intent of the Act to allow electronic signatures to comply with any law requiring documents to be “signed” or “subscribed” or that a person supply his “signature” thereto. The limited recognition therefore is relevant and affects the execution of the following documents: negotiable instruments (promissory notes, bills of exchange and checks; Section 1, Negotiable Instruments Law); holographic wills (Arts. 810, 812, and 813, Civil Code); the written inventory attached to an articles of partnership (Art. 1773, Civil Code);

articles of a limited partnership and amendments thereto (Arts. 1844 and 1865, Civil Code); a waiver of an incontestability clause in group life insurance policies (Sec. 228, Insurance Code); and, articles of incorporation and by-laws of a corporation (Secs. 14 and 46, Corporation Code). These documents may only be signed by an electronic signature complying with the requirements of Section 13 above or Section 8 of the Act. Failing that, the foregoing will either become invalid, infirm or suffer from some other adverse legal consequence.

Additionally, no document will be considered “signed” under Philippine law unless it also complies with the aforementioned provisions of the Act and the IRR. These include *all types of signed documents* such as contracts, agreements, deeds, affidavits, application forms, pleadings and waivers. The absence of any signature on these documents may not necessarily affect the underlying transaction. Note that contracts under Philippine law need not be embodied in any particular form nor signed.

However, the absence of a valid electronic signature certainly raises issues as to the inherent validity of the electronic document itself or of its contents. An admission of a particular fact contained in an electronic document may, for example, be denied legal effect if it is unsigned. For example, a person may admit his paternity of a child in a word processing file and for this purpose, may affix a digitized image of his manual signature. The electronic signature would certainly be invalid under the Act and the document will be considered “unsigned” under Philippine law. In such a case, it is uncertain if the contents of the electronic document may be relied upon say, by the child in a suit to establish paternity. On the one hand, it may be said that an unsigned document is a mere scrap of paper; upon the other,

it may be equally said that the mere lack of the signature does not necessarily invalidate the contents thereof or the information contained therein.

Introduction to Cryptograph and Digital Signatures. Since the only electronic signature recognized under the Act is a digital signature, it is important to discuss cryptography and public key infrastructure.

Cryptography is generally understood to encompass encryption and decryption. Encryption is the transformation of data such as plaintext, into an unintelligible format called cipher text that cannot be read without the appropriate "key". Decryption is the opposite of encryption and renders unintelligible data readable by the application of the "key". There are two popular types of cryptographic systems: secret key and public key.

In secret key cryptography, also known as symmetric cryptography, the same key is used for encryption and decryption. However, the use of secret keys proved to be inconvenient and entailed unnecessary expense. In response to these issues, public key cryptography was developed. In this system, also known as asymmetric cryptography, algorithms are used to create two mathematically-related keys. One key is kept by its owner and undisclosed (the "private key") while the other is published and made easily available on the network (the "public key"). Under this system, the sender can use his private key to encrypt a message and the receiver can use the sender's public key to decrypt the same. For ease of access, public keys are published together with the names of their owners in electronic directories readily accessible over the Internet. A party to an electronic contract need only refer to the directory to relate a particular public key to the identity of its owner.

Although the directories provide a name or identity associated with a public key, for pur-

poses of entering into transactions however there will still be concerns regarding the accuracy of the information in such directories. Hence, the need for a trusted third party to attest to the relationship between a public key and its owner. This third party is called a certification authority or "CA". Typically, the CA issues the public and private keys but only after the person to whom such keys are issued presents himself personally at the CA's offices to prove his identity. Once the CA has verified his identity, it will then issue a digital certificate identifying him to the public key. The creation of an open and public cryptographic system has been called the public key infrastructure – PKI for short.

Of particular interest are "digital signatures" which are essential in e-commerce transactions because of the role they play in the creation, validity and enforcement of electronic contracts. Digital signatures are not digitized or scanned images of a person's signature. It is, instead, a method by which a person's communication of an offer or consent (whether by e-mail or through a click of an "I Accept" button on an on-line session) can be independently verified for authenticity and integrity.

Here's how it works: if Pepe were to affix a digital signature to his e-mail contract, he must initially use a "hash" function to create a compressed form of the e-mail called the "message digest." Pepe then applies his private key to the message digest to encrypt the same. Thereafter, he sends the message digest and the e-mail to Pilar who then decrypts the message digest using Pepe's public key. Pilar then applies the same hash function to the e-mail which generates a second message digest and determines if the latter digest is identical with the message digest decrypted using Pepe's public key. If they are identical, then Pepe's signature is authenticated. If they are not

identical then this could mean that an error occurred during transmission or the message was altered.

The use of the hash function on the message and its comparison with the message digest decrypted from the Pepe's public key enables the Pilar to verify any alteration in the message during transit. This ensures message integrity. In addition, since the message digest was decrypted using the Pepe's public key, it denotes that it was encrypted using the Pepe's private key that is in his possession – a fact certified to by the Pepe's CA which issues a digital certificate. This proves that the message was sent by Pepe and by no one else — thus establishing the source of the same. Taken together, message integrity and identity form the basis for non-repudiation by Pepe. Such non-repudiation authenticates electronic documents to a degree sufficient to make parties liable thereon.

The ease by which electronic transactions can be proven using PKI can only spur the growth of e-commerce. As demonstrated, PKI raises electronic contracts to the same level as physical contracts as a method of proving the electronic transaction. Coupled with CAs of unquestioned integrity, PKI has the potential to enable transactions between total strangers without depriving them of remedies in case of breach. In the context of an open system such as the Internet, this would be invaluable.

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 elec-

tronic 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.

Presumptions. Note that the above presumptions will apply only if the electronic signature has been shown to have complied with the requirements of Section 13 above or Section 8 of the Act. In other words, the signature and the “method” specified under the Act must be proven before the presumptions arise.

Modes of Authentication

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, 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.

Authentication. The authentication referred to under this Section should be understood in relation to the authentication of private documents under the Rules of Court. For the purpose of their presentation in evidence, documents are either public or private (Section 19, Rule 132, Rules of Court). Public documents are among others, notarized documents and public records. As a rule, public documents need not be authenticated as a condition to their admission in evidence (Section 23, Rule 132, Rules of Court).

In contrast, before private documents are allowed into evidence, their due execution and authenticity must be established. This is done either by the testimony of a witness to the execution of the document or by evidence of the genuineness of the signature or handwriting of the document’s maker (Section 20 [a] and [b], Rule 132, Rules of Court).

The above-quoted Section provides suggestions as to the manner in which electronic evidence may be authenticated. It would not be unreasonable to suppose that if the electronic document qualifies as a public document, it need not be authenticated as provided above. This would be consistent with the provisions of the Rules of Court. Therefore, the above provision would be applicable mostly to electronic data messages which are private documents.

Note that the enumeration of the modes of authentication is not exhaustive. Parties presenting such evidence therefore are free to authenticate the same in any other manner.

Section 16. *Burden of Authenticating Electronic Documents or Electronic Data Messages.* The person seeking to introduce an electronic document or electronic data message in any legal proceeding has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic data message or electronic document is what the person claims it to be.

Authentication. In response to a question posed by Sen. Loren Legarda-Leviste as to who will perform the function of authentication, Sen. Magsaysay replied that the parties themselves may do so or in the alternative, engage the services of third-party authenticators such as credit card companies, certificate issuers and service providers.

Modes for Establishing Integrity

Section 17. *Method of Establishing the Integrity of an Electronic Document or Electronic Data Message.* 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.

Necessity for establishing integrity. This Section establishes a manner by which the integrity of an electronic data message or signature may be proven. Note that integrity is an essential element of an electronic "original" or "writing" under Sections 10 and 11 of the IRR.

The methods listed in this provision are by no means exclusive – other ways may be resorted to prove such integrity. On one extreme, this provision may altogether be ignored when proving the integrity.

Admissibility and Evidential Weight

Section 18. *Admissibility and Evidential Weight of Electronic Data Messages and Electronic Documents.* For evidentiary purposes, an electronic document or electronic data message shall be the functional equivalent of a written document under existing laws. 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.

The 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.

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 com-

municated, the reliability of the manner in which its originator was identified, and other relevant factors shall be given due regard.

Origin. This provision is based primarily upon Article 9 of the Model Law.

Admissibility. The Act provides that electronic documents are the functional equivalent of paper documents for evidentiary purposes. In plain terms, this means that the provisions of the Rules of Court on documentary evidence apply with equal force in the presentation of electronic documents.

As discussed above (in relation to Section 15 of the IRR), the Rules of Court categorizes documents as public or private. Public documents are: (a) official government records; (b) notarized documents; and (c) public records of private documents required by law to be entered therein (Section 19, Rule 132, Rules of Court). All other documents are private (*Ibid.*).

From the standpoint of presenting evidence, the main difference between public and private documents is that the former need not be authenticated and are immediately admissible (Section 23, Rule 132, Rules of Court). Private documents, on the other hand, must be authenticated in the manner provided for in Section 20, Rule 132 of the Rules.

As applied to the Act, electronic documents which qualify as public documents would therefore be readily admissible and need no authentication. The reverse is true for electronic documents which are private – they need to be authenticated either in accordance with the Rules of Court or Section 15 of the IRR. As noted above, the provisions of the IRR are not exhaustive as to the modes of authenticating electronic documents.

Evidential Weight. The final paragraph of Section 18 is culled from paragraph (2), Article 9 of the Model Law. It provides a

useful guide as regards the assessment of the evidential weight of an electronic data message (§71, Guide).

Section 19. *Proof by Affidavit and Cross-Examination.* The matters referred to in Section 12 of the Act on admissibility and evidentiary weight, and Section 9 of the Act on the presumption of integrity of electronic signatures, may be presumed to have been established by an affidavit given to the best of the deponent's or affiant's personal knowledge subject to the rights of parties in interest to cross-examine such deponent or affiant as a matter of right. Such right of cross-examination may likewise be enjoyed by a party to the proceedings who is adverse in interest to the party who has introduced the affidavit or has caused the affidavit to be introduced.

Any party to the proceedings has the right to cross-examine a person referred to in Section 11, paragraph 4, and sub-paragraph (c) of the Act.

Recommended Mode of Presenting Evidence. By this provision, all matters relating to the admissibility and evidential weight of electronic evidence may be set forth in an affidavit. This simplifies the presentation of electronic evidence in that the party presenting or offering the same is freed from the drawn out process of the direct examination of witnesses since the affidavit performs this function.

From the standpoint of a person who or entity which processes or handles large amounts of electronic data and are therefore more likely to be hailed into court as witnesses to establish a particular fact with respect to such data, this provision can save them precious manhours as standardized affidavit forms may be used. All that remains then would be the cross-examination on the affidavit. It is therefore advisable for such entities to formulate and draft such standard forms for future use and reference.

Retention of Electronic Data Message and Electronic Document

Section 20. Retention of Electronic Data Message and Electronic Document. Notwithstanding any provision of law, rule or regulation to the contrary:

a) The requirement in any provision of law that certain documents be retained in their original form is satisfied by retaining them in the form of an electronic data message or electronic document which:

(i) Remains accessible so as to be usable for subsequent reference;

(ii) Is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to accurately represent the electronic data message or electronic document generated, sent or received; and,

(iii) Where applicable, enables the identification of its originator and addressee, as well as the determination of the date and the time it was sent or received.

b) The requirement referred to in paragraph (a) is satisfied by using the services of a third party, provided that the conditions set forth in subparagraphs (i), (ii) and (iii) of paragraph (a) are met.

c) Relevant government agencies tasked with enforcing or implementing applicable laws relating to the retention of certain documents may, by appropriate issuances, impose regulations to ensure the integrity, reliability of such documents and the proper implementation of Section 13 of the Act.

Source of Provision. This provision is based on Article 10 of the Model Law.

Additional language (*i.e.*, the words “where applicable”) was inserted in subparagraph (iii) of paragraph (a) in order to align the provision with the Model Law. The task force deemed this to be a valid interpretation consistent with Section 37 of the Act which mandates that all statutory construction must give due regard to the Act’s international origin.

Retention. By this provision, all private individuals and entities will be allowed to keep government records in electronic forms. This refers, among others, to invoices and financial records required to be kept pursuant to the Tax Code. Pursuant to the Act, businesses may now digitize (*i.e.*, either by scanning or manual data encoding) such information and keep them in electronic form. Filing cabinets will now be replaced by CD-ROMs and computers. This is expected to spur the growth of businesses offering digital imaging and encoding as companies move to reclaim precious office space now occupied by bulky filing cabinets.

In relation to the Philippine eGovernment. Paragraph (c) was inserted into the IRR in order to harmonize this with the provision mandating the Philippine government to conduct its business electronically (Sec. 27, Act). It is expected that the government will not meet the two (2) year deadline set by the Act.

In the meantime, the above provision on retention is immediately effective and private entities will be allowed to keep government records in electronic form. Obviously, such records are important to the government agencies because the records allow them to conduct audits and other investigations. If the entities under regulation adopt conflicting or different standards in storing its records electronically, it may seriously impair the government’s ability to perform its regulatory functions as it might become difficult to deal with such conflicting standards. As a result, it is more reasonable to allow such agencies to issue rules and regulations governing the manner in which such records are kept in electronic form.

Meanwhile, it is suggested that if a private entity wishes to digitize its records, it should inquire with the relevant government agency to ensure compliance with such agency’s plans.

Chapter III - Communication of Electronic Data Messages and Electronic Documents

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.

Philippine Contract Law (Spiritual System). It has been said that the main objective of the Act is to legalize electronic contracts and transactions. However, under Philippine law, “a contract is a meeting of minds between two persons whereby one binds himself, with respect to the other, to give something or to render some service” (Art. 1305, Civil Code). Contracts are consensual in nature and therefore perfected upon the absolute acceptance of a definite offer (*Asuncion v. Court of Appeals*, 238 SCRA 602 [1994]).

In addition, the Philippine Civil Code adheres to the spiritual system where contracts are valid if made in any way that indicates that the party wished to be bound. In contrast, a formalist system considers contracts non-binding if they fail to comply with prescribed ceremonial requirements. Article 1356 of the Civil Code states that “(c)ontracts shall be obligatory, in whatever form they may have been entered into, provided all the essential requisites for their validity are present.” On the basis of the foregoing, the High

Court has repeatedly upheld the validity of contracts evidenced only by testimonial evidence (*Thunga Chui v. Que Bentec*, 2 Phil 561; *Alcantara v. Alineo*, 8 Phil. 111; *Peterson v. Azada*, 8 Phil. 432). Generally, therefore, a contract under Philippine law will be valid in whatever form it may be found whether it be oral, paper-based or for that matter, electronic.

Recognition of Electronic Contracts. There is also some basis to say that Philippine law recognizes electronic contracts in the absence of the Act. Article 17 of the Civil Code provides that the forms and solemnities of contracts shall be governed by the laws of the country where the contract was executed. By codal provision, therefore, the Philippines follows the *lex loci contractus* rule. In this regard, the Supreme Court has had occasion to rule that a power of attorney executed in Germany, must be tested as to its formal validity by the laws of that country and not the Civil Code (*German & Co. v. Donaldson, Sim & Co.*, 1 Phil 63 [1901]). In other words, if the law where the electronic contract was entered into recognizes such form of agreements, those electronic agreements are extrinsically valid in the Philippines. Assuming further that such agreements are likewise intrinsically valid, then those electronic contracts would be valid in all respects under Philippine law.

In light of this conclusion, some are of the view that Philippine law did not need any new legislation to accommodate electronic commerce. Any issue respecting the applicability of existing law to electronic documents and signatures could properly be resolved by the courts as cases on electronic commerce come before them.

On the other hand, the limitations of the judicial system should also be taken into consideration. It may be unable to create a stable environ-

ment necessary for the growth of electronic commerce. Inconsistent jurisprudence may even have a destabilizing effect and inadvertently lead to a decline in electronic commerce. This has, of course, become academic with the passage of the Act.

Validity of Electronic Contracts. This provision explicitly validates electronic contracts under Philippine law. Note, however, that the Act does not amend the law on contracts but merely allows the requisite elements thereof to be expressed in electronic form. Under Philippine law, the external manifestation of a contract is the meeting of the offer and the acceptance upon the thing and the cause which are to constitute the contract (Art. 1319, Civil Code). The external elements are therefore the offer and acceptance.

It should also be emphasized that the Act covers not merely the cases in which both the offer and the acceptance are communicated electronically, but also cases in which only the offer or only the acceptance is communicated electronically (§178, Guide). In other words, an e-mail acceptance to a handwritten offer can be used as the basis to prove the existence of the contract.

Contract Law – Intrinsic Validity. Nothing in this provision of the Act or IRR should be deemed to have amended the law on contracts insofar as intrinsic validity is concerned. Contracts are either valid or invalid based on the Civil Code provisions on Obligations and Contracts. In addition, illegal provisions such as *pactum commissorium*, and other terms contrary to law, morals, public order or public policy will receive equal treatment even though appearing in an electronic document. As mentioned elsewhere, the Act intends only to amend the law with respect to the form of documents and transactions.

Section 22. Consummation of Electronic Transactions with

***Banks.* Electronic transactions made through networking among banks, or linkages thereof with other entities or networks, and vice versa, shall be deemed consummated under rules and regulations issued by the Bangko Sentral under the succeeding paragraph hereunder, upon the actual dispensing of cash or the debit of one account and the corresponding credit to another, whether such transaction is initiated by the depositor or by an authorized collecting party; Provided, that the obligation of one bank, entity, or person similarly situated to another arising therefrom shall be considered absolute and shall not be subjected to the process of preference of credits; Provided, however, that the foregoing shall apply only to transactions utilizing the Automated Teller Machine switching network.**

Without prejudice to the foregoing, all electronic transactions involving banks, quasi-banks, trust entities, and other institutions which under special laws are subject to the supervision of the Bangko Sentral ng Pilipinas shall be covered by the rules and regulations issued by the same pursuant to its authority under Section 59 of Republic Act No. 8791 (The General Banking Act), Republic Act No. 7653 (the Charter of the Bangko Sentral ng Pilipinas) and Section 20, Article XII of the Constitution.

Backgrounder on the Provision. This provision appeared in the House version of the Act and was adopted by the Bicameral Conference Committee. It was suggested by an Automated Teller Machine (“ATM”) network group to address a specific problem they had encountered with respect to a bank which recently closed. For convenience, we shall refer to such bank as Bank A.

Bank A’s Board of Directors declared it closed as of 6:00 p.m. of a particular day. However, Bank A’s ATM machines were operational until 10:00 p.m. Hence, its depositors were able

to withdraw not only from Bank A's ATMs but those of other banks which were members of the same ATM network. Cash was actually dispensed and the accounts of these cardholders with Bank A were duly debited. Meanwhile, Bank A was in no position to settle its obligations with the members of the ATM network citing its closure.

A corresponding issue arose with respect to the nature of Bank A's liability to the other banks. On the one hand, Bank A held that the other banks merely stood as unsecured creditors and pursuant to the Philippine insolvency law, such creditors stand as one of the lowest in the hierarchy of creditors. Hence, the banks had very little chance of recovery. The ATM network banks, however, believed that since Bank A's depositors received cash and their accounts were debited, Bank A benefited from the transaction. It should be noted that under Philippine law, bank depositors are deemed to be creditors of a bank. In short, when the total deposits of Bank A were decreased by the ATM withdrawals, its total liabilities to depositors were likely decreased. In which case, the ATM network lawyers held the position that Bank A was unjustly enriched and the sums due them from Bank A were held by the latter in trust for them. If that were the case, then the banks would be immediately entitled to the remittance of the sum due them and the sum held by Bank A in trust for them would no longer be the subject of insolvency proceedings.

Unfortunately, the provision which appeared in Section 16(2) of the Act was as follows:

"Electronic transactions made through networking among banks, or linkages thereof with other entities or networks, and vice versa, shall be deemed consummated upon the actual dispensing of cash or the debit of one account and the corresponding credit to another, whether such transaction is ini-

tiated by the depositor or by an authorized collecting party: *Provided*, that the obligation of one bank, entity, or person similarly situated to another arising therefrom shall be considered absolute and shall not be subjected to the process of preference of credits."

The provision achieved the goal of excluding Bank A's obligations from the insolvency proceedings by declaring the obligation to pay absolute and free from the process of preferences of credits. However, the provision inadvertently provided for modes of perpetrating fraud through electronic banking.

In sum, the provision states that the obligation of a bank to pay upon an electronic transaction or order is *absolute*. Hence, if a depositor sends an electronic authorization to pay a certain amount to a third party, the bank is in no position to resist the obligation to pay. Since it is absolute, it may be countermanded only by the person giving such instruction – third parties who may be prejudiced thereby would have no recourse.

Problems with this provision were apparent from the beginning. Consider a situation involving an insolvent company. The bankrupt company could send electronic instructions to the bank to make payments to foreign accounts of its principal shareholders or of preferred creditors. If the company closes after sending the electronic instruction and files for insolvency, the unpaid creditors and even the insolvency court would be unable to stop the payment by the bank because the Act provides that its obligation to remit the funds is *absolute* and shall not be subjected to the process of preferences of credits. The provision of the Act may therefore be used to facilitate fraud with the unwitting and involuntary participation of the banks.

Realizing this, the Bangko Sentral ng Pilipinas ("BSP") moved to insert the amendments which now appear in Sec-

tion 22 above. In short, they limited the application of the provision only to ATM networks and stressed the BSP's authority vis-à-vis banks and other financial institutions – leaving open the possibility that the BSP will issue circulars to prevent the potential abuse of Section 16(2) of the Act.

Section 23. Recognition by Parties of Electronic Data Message. *As between the originator and the addressee of an electronic data message or electronic document, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the ground that it is in the form of an electronic data message or electronic document.*

Source. This is based on Article 12 of the Model Law.

Attribution of Electronic Data Message and Electronic Document

Section 24. Origin of Electronic Data Message. *An electronic data message or electronic document is that of the originator if it was sent by the originator himself.*

Section 25. Origin of Electronic Data Message Not Personally Sent by an Originator. *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 and communications system programmed by, or on behalf of the originator to operate automatically.*

Section 26. When an Originator May Be Bound By an Electronic Data Message. *As between the originator and the addressee, an addressee is entitled to regard an electronic data message or elec-*

tronic document as being that of the originator, and to act on that assumption, if:

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

b) the 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 or electronic documents as his own.

The provisions of this Section do not exclude other instances or circumstances when an originator may be bound by the reliance and consequent action of an addressee respecting an electronic data message, which purports to have been that of the originator.

Section 27. *When an Originator May Not Be Bound By an Electronic Data Message.* As between the originator and the addressee, an addressee is not entitled to regard an electronic data message as being that of the originator, and to act on that assumption:

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

b) in a case within paragraph (b) Section 26 of these Rules, at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the electronic data message or electronic document was not that of the originator.

The provisions of this Section do not exclude other instances or circumstances when an originator may not be liable for the reliance and consequent action of an addressee respecting an electronic data message, which purports to have been that of the originator.

Source. This is based on Article 13 of the Model Law.

Attribution. The provisions on attribution were intended to impose liability upon originators and addressees with respect to electronic data messages. This liability rests on the principle that a party is entitled to rely (or not to rely) upon the contents of an electronic data message and has the authority to take the appropriate action.

For example, if the e-mail of Bob authorized Alice to purchase shares of stock in say, Apple and the situation falls within Section 26 above, then Bob will be liable for Alice's subsequent purchase of the shares even though Bob meant to buy shares in Snapple. But if the situation fell within Section 27, Alice will have to bear the loss as Bob will be able to disown the electronic instructions.

It should be noted that the parties are free to stipulate upon terms other than those set forth in the above sections. Furthermore, even in the absence of such an agreement, the situations set forth in the said sections are by no means exhaustive. There may be other instances or circumstances in which a party may incur (or be absolved from) liability pursuant to an electronic data message.

Separate Receipt of and Error on Electronic Data Message and Electronic Document

Section 28. *Assumption Regarding Receipt of Separate Electronic Data Messages.* The addressee is entitled to regard each electronic data message or electronic document received as a separate electronic data message or electronic document and to act on that assumption, except to the extent that it duplicates another electronic data message or electronic document and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the electronic data message or elec-

tronic document was a duplicate.

Section 29. *Error on Electronic Data Message or Electronic Document.* The addressee is entitled to regard the electronic data message or electronic document received as that which the originator intended to send, and to act on that assumption, unless the addressee knew or should have known, had the addressee exercised reasonable care, used the appropriate procedure or applied an agreed procedure:

a) That the transmission resulted in any error therein or in the electronic data message or electronic document when the latter enters the designated information and communications system; or,

b) That electronic data message or electronic document is sent to an information and communications system which is not so designated by the addressee for the purpose.

Source. This is based on Article 13 of the Model Law.

Rules are not Exhaustive. The rules set forth in Sections 28 and 29 are not exhaustive. They are guideposts as to how these issues are resolved but do not exclude other circumstances or rules that may evolve in the future. The courts and common usage are therefore expected to enhance these rules.

Dispatch and Receipt of Electronic Data Message and Electronic Document

Section 30. *Agreement on Acknowledgment of Receipt of Electronic Data Messages or Electronic Documents.* The following rules shall apply where, on or before sending an electronic data message or electronic document, the originator and the addressee have agreed, or in that electronic document or electronic data message, the originator has requested, that receipt of the electronic document or electronic data message be acknowledged:

a) Where the originator has not agreed with the addressee that the acknowledgment be given in a particular form or by a particular method, an acknowledgment may be given by or through any communication by the addressee, automated or otherwise, or any conduct of the addressee, sufficient to indicate to the originator that the electronic data message or electronic document has been received.

b) Where the originator has stated that the effect or significance of the electronic data message or electronic document is conditional on receipt of the acknowledgment thereof, the electronic data message or electronic document is treated as though it has never been sent, until the acknowledgment is received.

c) Where the originator has not stated that the effect or significance of the electronic data message or electronic document is conditional on receipt of the acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator may give notice to the addressee stating that no acknowledgment has been received and specifying a reasonable time by which the acknowledgment must be received; and if the acknowledgment is not received within the time specified, the originator may, upon notice to the addressee, treat the electronic document or electronic data message as though it had never been sent, or exercise any other rights it may have.

Source. This is based on Article 14 of the Model Law.

Note. This provision applies only in instances where the parties have either agreed or the originator has requested an acknowledgment of receipt. In the absence of either, then the following provisions will apply.

Section 31. *Time of Dispatch of Electronic Data Message or Electronic Document.* Unless otherwise agreed between the origi-

nator and the addressee, the dispatch of an electronic data message or electronic document occurs when it enters an information and communications system outside the control of the originator or of the person who sent the electronic data message or electronic document on behalf of the originator.

Source. This is based on Article 15 of the Model Law.

Dispatch. This provision states that dispatch occurs when the electronic data message enters an information and communications system outside the control of the originator. This applies readily to Internet e-mail where the time of dispatch would be the time of its transmission from the sender's ISP. However, the time of dispatch of an e-mail sent to an addressee within a local area network or for that matter the same ISP, is uncertain because it may be said that the e-mail never enters a system outside the control of the originator. It is therefore suggested that internal e-mail and other communications systems conform to a set of rules which will determine the time of dispatch of electronic data messages.

Section 32. *Time of Receipt of Electronic Data Message or Electronic Document.* Unless otherwise agreed between the originator and the addressee, the time of receipt of an electronic data message or electronic document is as follows:

a) If the addressee has designated an information and communications system for the purpose of receiving electronic data message or electronic document, receipt occurs at the time when the electronic data message or electronic document enters the designated information and communications system; Provided, however, that if the originator and the addressee are both participants in the designated information and communications system, receipt occurs at the time when the electronic data message or electronic document is retrieved by the addressee.

b) If the electronic data message or electronic document is sent

to an information and communications system of the addressee that is not the designated information and communications system, receipt occurs at the time when the electronic data message or electronic document is retrieved by the addressee.

c) If the addressee has not designated an information and communications system, receipt occurs when the electronic data message or electronic document enters an information and communications system of the addressee.

These rules apply notwithstanding that the place where the information and communications system is located may be different from the place where the electronic data message or electronic document is deemed to be received.

Source. This is based on Article 15 of the Model Law.

Time of Receipt. In the case of subparagraph (a), time of dispatch and receipt may occur at the same time.

Retrieve. There is some leeway to interpret the word "retrieve". Some hold that it refers to the time when the e-mail is downloaded by the addressee from the server even though the messages remain unread. Meanwhile, others claim "retrieve" should refer to the time the mail is actually read or opened by the addressee.

Significance. Time of receipt has legal significance in some instances such as when a notice is required to be served within a particular time limit. Should there be a dispute, these provisions may provide some guidance.

Section 33. *Place of Dispatch and Receipt of Electronic Data Message or Electronic Document.* Unless otherwise agreed between the originator and the addressee, an electronic data message or electronic document is deemed to be dispatched at the place where the originator has its place of business and received at the place where the addressee has its place of business. This rule shall apply even if the originator or addressee had used

a laptop or other portable device to transmit or receive his electronic data message or electronic document. This rule shall also apply to determine the tax situs of such transaction 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.

For the purpose hereof -

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

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

c) The "usual place of residence" in relation to a body corporate, which does not have a place of business, means the place where it is incorporated or otherwise legally constituted.

Nothing in this Section shall be deemed to amend the rules of private international law.

Source. This is based on Article 15 of the Model Law.

Presumption as to the Place of Receipt and Dispatch. This provision was based on Article 15(4) of the Model Law. It was recognized that given the distributed nature of the Internet, it would not be proper to determine the place of receipt and dispatch of electronic data messages based upon the location of the servers where the said message was first sent by the originator or retrieved by the addressee. Since originators and addressees can easily change the location of said servers, it would only create further confusion. Hence, the above rule sets the place of receipt and dispatch to the party's place of business or failing that, his habitual residence. This way, the location of the servers becomes irrelevant.

Note further that this provision may be subject to the

agreement of the parties involved.

Relevance of the Provision. This provision is important in the context of legal requirements respecting the service or presentation of documents at a particular location. For example, substituted summons may be served at the defendant's place of business. Assuming electronic summons were acceptable, then the place of service may be established in accordance with this provision.

Private International Law. The final sentence was inserted to clarify that the provision is not intended to determine which law will apply to a particular electronic data message. This arises from the simple fact that the application of the rule usually reveals two (2) locations – the place of dispatch and the place of receipt. For example, an e-mail from a Philippine corporation to a US corporation may be said to have been dispatched in Manila and received in Seattle. Given this information, it is impossible to determine which law applies to either the electronic data message or the underlying transaction.

Tax Situs. The provision on *tax situs* appears in this Section but it is submitted that it is dead letter law. As stated above, the application of this provision always reveals at most two (2) places – the place of receipt and the place of dispatch. This information does not reveal either the jurisdiction of the transaction nor *tax situs* thereof. In fact, it points to alternative national laws that may apply but the rule will not determine *tax situs*.

Security Methods

Section 34. Choice of Security Methods. Subject to applicable laws and/or rules and guidelines promulgated by the Department of Trade and Industry and other appropriate government agencies, parties to any electronic transaction shall be free to determine the type and level of electronic data

message or electronic document security needed, and to select and use or implement appropriate technological methods that suit their needs.

Source. This provision was inspired by the Organisation for Economic Cooperation and Development's (OECD) Guidelines for Cryptography Policy (Paragraph 2, Part 5) adopted on December 19, 1997. It was suggested for inclusion into Committee Report No. 34 by the Philippine Internet Commerce Society (PICS) and made its way into SB 1523.

Freedom of Choice. This provision allows parties to utilize any security or authentication method appropriate to suit their needs. This refers primarily to public key encryption technologies or the use of digital signatures. Other than that, parties may use other information security measures such as firewalls, intruder detection systems and virtual private networks. Another example would be technologies to determine the exact time of receipt and dispatch of electronic data messages.

During the Senate interpellation of SB 1523 (later SB 1902), Sen. Magsaysay, in response to a question from Sen. Robert Jaworski, stated that parties may use encryption technologies to ensure the integrity and unalterability of the terms and conditions of electronic contracts.

Government Regulation. This serves as the basis for the DTI or other government agency to issue rules and regulations over the use of encryption technologies particularly, public key encryption technologies. The DTI for example could issue rules on the accreditation of certificate authorities or CAs and determine the liability of different parties for such things as lost private keys and stale revocation certificates. Although these matters could have been included in the Act, it was deferred given the complexity of the issues and the urgent need for the law. In-

stead, the authority was vested with the DTI to fill in the gaps by issuing the appropriate rules and regulations when needed.

Limits. This freedom is limited by rules and regulations of government agencies. Security methods typically utilize encryption technologies which, if they are to be effective, are computationally infeasible to crack. The usage of these encryption technologies raise national security issues since it restricts the ability of government to take certain defensive actions against threats. For example, a militant group could utilize encryption to maintain a secure and private communications network via the Internet. Their messages may include instructions or orders to commit acts of terrorism that lead to destabilization. The irony is that these groups would be using telecommunications facilities provided under franchise from the Philippine government. Different countries are considering various ways to address this issue. The US Government for a time advocated a key escrow whereby access to keys were given to law enforcement agencies immediately upon the government's procurement of a warrant. This was heavily opposed until later abandoned.

PART III

ELECTRONIC COMMERCE IN CARRIAGE OF GOODS

Section 35. *Actions Related to Contracts of Carriage of Goods.* Without derogating from the provisions of Part Two of the Act, this Part of the Rules applies to any action in connection with, or in pursuance of, a contract of carriage of goods, including but not limited to:

- (a) (i) furnishing the marks, number, quantity or weight of goods;
- (ii) stating or declaring the nature or value of goods;
- (iii) issuing a receipt for goods;

(iv) confirming that goods have been loaded;

(b) (i) notifying a person of terms and conditions of the contract;

(ii) giving instructions to a carrier;

(c) (i) claiming delivery of goods;

(ii) authorizing release of goods;

(iii) giving notices of loss of, or damage to goods;

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

(e) undertaking to deliver goods to a named person or a person authorized to claim delivery;

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

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

Section 36. *Transport Documents.* (1) Subject to paragraph (3), where the law requires that any action referred to in the immediately preceding Section be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more electronic data messages or electronic documents. The transport documents referred to herein shall include, but not be limited to, those enumerated in Annex "1" hereof. Concerned agencies such as, but not limited to, the DTI, Department of Finance, DOTC, Philippine Ports Authority and other port authorities, shall, within their respective mandates, issue appropriate rules and guidelines with respect to transport documents as provided herein.

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

(3) If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the

right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more electronic data messages or electronic documents: Provided, That a reliable method is used to render such electronic data messages or electronic documents unique.

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

(5) Where one or more electronic data messages or electronic documents are used to effect any action in subparagraphs (f) and (g) of Section 25 of the Act, no paper document used to effect any such action is valid unless the use of electronic data message or electronic document has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of electronic data messages or electronic documents by paper documents shall not affect the rights or obligations of the parties involved.

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

Source. This entire chapter is almost a reproduction of Articles 16 and 17 of the Model Law.

Comments. For this purpose, the following paragraphs from the Guide containing comments on the said provisions of the Model Law are hereby reproduced for reference:

109. The adoption of a specific set of rules dealing with specific uses of electronic commerce, such as the use of EDI messages as substitutes for transport documents does not imply that the other provisions of the Model Law are not applicable to such documents. In particular, the provisions of part two, such as articles 16 and 17 concerning transfer of rights in goods, presuppose that the guarantees of reliability and authenticity contained in articles 6 to 8 of the Model Law are also applicable to electronic equivalents to transport documents. Part two of the Model Law does not in any way limit or restrict the field of application of the general provisions of the Model Law.

x x x x x x x x x

110. In preparing the Model Law, the Commission noted that the carriage of goods was the context in which electronic communications were most likely to be used and in which a legal framework facilitating the use of such communications was most urgently needed. Articles 16 and 17 contain provisions that apply equally to non-negotiable transport documents and to transfer of rights in goods by way of transferable bills of lading. The principles embodied in articles 16 and 17 are applicable not only to maritime transport but also to transport of goods by other means, such as road, railroad and air transport.

Article 16. Actions related to contracts of carriage of goods
[Section 35 of the IRR]

111. Article 16, which establishes the scope of chapter I of part two of the Model Law, is broadly drafted. It would encompass a wide variety of documents used in the context of the carriage of goods, including, for example, charter-parties. In the preparation of the Model Law, the Commission found that, by dealing comprehensively with contracts of carriage of goods, article 16 was consistent with the need to cover all transport documents, whether negotiable or

non-negotiable, without excluding any specific document such as charter-parties. It was pointed out that, if an enacting State did not wish chapter I of part two to apply to a particular kind of document or contract, for example if the inclusion of such documents as charter-parties in the scope of that chapter was regarded as inappropriate under the legislation of an enacting State, that State could make use of the exclusion clause contained in paragraph (7) of article 17.

112. Article 16 is of an illustrative nature and, although the actions mentioned therein are more common in maritime trade, they are not exclusive to such type of trade and could be performed in connection with air transport or multimodal carriage of goods.

[References omitted]

Article 17. Transport documents

[Section 36 of the IRR]

113. Paragraphs (1) and (2) are derived from article 6. In the context of transport documents, it is necessary to establish not only functional equivalents of written information about the actions referred to in article 16, but also functional equivalents of the performance of such actions through the use of paper documents. Functional equivalents are particularly needed for the transfer of rights and obligations by transfer of written documents. For example, paragraphs (1) and (2) are intended to replace both the requirement for a written contract of carriage and the requirements for endorsement and transfer of possession of a bill of lading. It was felt in the preparation of the Model Law that the focus of the provision on the actions referred to in article 16 should be expressed clearly, particularly in view of the difficulties that might exist, in certain countries, for recognizing the transmission of a data message as functionally equivalent to the physical transfer of goods, or to

the transfer of a document of title representing the goods.

114. The reference to "one or more data messages" in paragraphs (1), (3) and (6) is not intended to be interpreted differently from the reference to "a data message" in the other provisions of the Model Law, which should also be understood as covering equally the situation where only one data message is generated and the situation where more than one data message is generated as support of a given piece of information. A more detailed wording was adopted in article 17 merely to reflect the fact that, in the context of transfer of rights through data messages, some of the functions traditionally performed through the single transmission of a paper bill of lading would necessarily imply the transmission of more than one data message and that such a fact, in itself, should entail no negative consequence as to the acceptability of electronic commerce in that area.

115. Paragraph (3), in combination with paragraph (4), is intended to ensure that a right can be conveyed to one person only, and that it would not be possible for more than one person at any point in time to lay claim to it. The effect of the two paragraphs is to introduce a requirement which may be referred to as the "guarantee of singularity". If procedures are made available to enable a right or obligation to be conveyed by electronic methods instead of by using a paper document, it is necessary that the guarantee of singularity be one of the essential features of such procedures. Technical security devices providing such a guarantee of singularity would almost necessarily be built into any communication system offered to the trading communities and would need to demonstrate their reliability. However, there is also a need to overcome requirements of law that the guarantee of singularity be demonstrated, for ex-

ample in the case where paper documents such as bills of lading are traditionally used. A provision along the lines of paragraph (3) is thus necessary to permit the use of electronic communication instead of paper documents.

116. The words “one person and no other person” should not be interpreted as excluding situations where more than one person might jointly hold title to the goods. For example, the reference to “one person” is not intended to exclude joint ownership of rights in the goods or other rights embodied in a bill of lading.

117. The notion that a data message should be “unique” may need to be further clarified, since it may lend itself to misinterpretation. On the one hand, all data messages are necessarily unique, even if they duplicate an earlier data message, since each data message is sent at a different time from any earlier data message sent to the same person. If a data message is sent to a different person, it is even more obviously unique, even though it might be transferring the same right or obligation. Yet, all but the first transfer might be fraudulent. On the other hand, if “unique” is interpreted as referring to a data message of a unique kind, or a transfer of a unique kind, then in that sense no data message is unique, and no transfer by means of a data message is unique. Having considered the risk of such misinterpretation, the Commission decided to retain the reference to the concepts of uniqueness of the data message and uniqueness of the transfer for the purposes of Article 17, in view of the fact that the notions of “uniqueness” or “singularity” of transport documents were not unknown to practitioners of transport law and users of transport documents. It was decided, however, that this Guide should clarify that the words “a reliable method is used to render such data message or messages

unique” should be interpreted as referring to the use of a reliable method to secure that data messages purporting to convey any right or obligation of a person might not be used by, or on behalf of, that person inconsistently with any other data messages by which the right or obligation was conveyed by or on behalf of that person.

118. Paragraph (5) is a necessary complement to the guarantee of singularity contained in paragraph (3). The need for security is an overriding consideration and it is essential to ensure not only that a method is used that gives reasonable assurance that the same data message is not multiplied, but also that no two media can be simultaneously used for the same purpose. Paragraph (5) addresses the fundamental need to avoid the risk of duplicate transport documents. The use of multiple forms of communication for different purposes, e.g., paper-based communications for ancillary messages and electronic communications for bills of lading, does not pose a problem. However, it is essential for the operation of any system relying on electronic equivalents of bills of lading to avoid the possibility that the same rights could at any given time be embodied both in data messages and in a paper document. Paragraph (5) also envisages the situation where a party having initially agreed to engage in electronic communications has to switch to paper communications where it later becomes unable to sustain electronic communications.

119. The reference to “terminating” the use of data messages is open to interpretation. In particular, the Model Law does not provide information as to who would effect the termination. Should an enacting State decide to provide additional information in that respect, it might wish to indicate, for example, that, since electronic commerce is usually based on the agreement of the parties, a decision

to “drop down” to paper communications should also be subject to the agreement of all interested parties. Otherwise, the originator would be given the power to choose unilaterally the means of communication. Alternatively, an enacting State might wish to provide that, since paragraph (5) would have to be applied by the bearer of a bill of lading, it should be up to the bearer to decide whether it preferred to exercise its rights on the basis of a paper bill of lading or on the basis of the electronic equivalent of such a document, and to bear the costs for its decision.

120. Paragraph (5), while expressly dealing with the situation where the use of data messages is replaced by the use of a paper document, is not intended to exclude the reverse situation. The switch from data messages to a paper document should not affect any right that might exist to surrender the paper document to the issuer and start again using data messages.

121. The purpose of paragraph (6) is to deal directly with the application of certain laws to contracts for the carriage of goods by sea. For example, under the Hague and Hague-Visby Rules, a contract of carriage means a contract that is covered by a bill of lading. Use of a bill of lading or similar document of title results in the Hague and Hague-Visby Rules applying compulsorily to a contract of carriage. Those rules would not automatically apply to contracts effected by one or more data message. Thus, a provision such as paragraph (6) is needed to ensure that the application of those rules is not excluded by the mere fact that data messages are used instead of a bill of lading in paper form. While paragraph (1) ensures that data messages are effective means for carrying out any of the actions listed in Article 16, that provision does not deal with the substantive rules of law that might apply to a contract contained in, or evidenced by, data messages.

122. As to the meaning of the phrase "that rule shall not be inapplicable" in paragraph (6), a simpler way of expressing the same idea might have been to provide that rules applicable to contracts of carriage evidenced by paper documents should also apply to contracts of carriage evidenced by data messages. However, given the broad scope of application of Article 17, which covers not only bills of lading but also a variety of other transport documents, such a simplified provision might have had the undesirable effect of extending the applicability of rules such as the Hamburg Rules and the Hague-Visby Rules to contracts to which such rules were never intended to apply. The Commission felt that the adopted wording was more suited to overcome the obstacle resulting from the fact that the Hague-Visby Rules and other rules compulsorily applicable to bills of lading would not automatically apply to contracts of carriage evidenced by data messages, without inadvertently extending the application of such rules to other types of contracts.

[References omitted]

PART IV

ELECTRONIC TRANSACTIONS IN GOVERNMENT

Chapter I - Government Use of Data Mes- sages, Electronic Documents and Electronic Signatures

Section 37. Government Use of Electronic Data Messages, Electronic Documents and Electronic Signatures. Notwithstanding any law to the contrary, within two (2) years from the date of the effectivity of the 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 submit-

ted, 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

d) 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 -

(1) the manner and format in which such electronic data messages or electronic documents shall be filed, created, retained or issued;

(2) 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;

(3) 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;

(4) 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;

(5) other attributes required of electronic data messages or electronic documents or payments; and

(6) the full or limited use of the documents and papers for compliance with the government require-

ments;

Provided, That the 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. 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 aforementioned 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.

Source. This provision is based on Section 47 of the ETA. Sen. Magsaysay suggested the two (2) year deadline to highlight the urgent need for government to implement or adopt electronic means of performing its functions.

The Philippine eGovernment. If this provision is strictly complied with, the entire Philippine government should be able to perform all its functions electronically within two (2) years. It is widely recognized however that the two (2) year deadline set by the Act is unrealistic. Therefore, it is unlikely that the same will be strictly enforced.

Section 38. Principles Governing Government Use of Electronic Data Messages, Electronic Documents and Electronic Signatures. The following principles shall govern the implementation of Section 27 of the Act and shall be mandatory upon all departments, bureaus, offices and agencies of the government, as well as all government-owned and-controlled corporations:

a) **Technology Neutrality.** All solutions implemented shall neither favor a particular technology over another nor discriminate against or in favor of particular vendors of technology.

b) **Interoperability.** All implementation of technological solutions shall ensure the interoperability of systems forming part of the government network.

c) **Elimination of Red Tape.** Government processes shall be re-examined and if appropriate, simplified or re-engineered to maximize the functionality of technology and to eliminate unnecessary delays in the delivery of governmental services.

d) **Security Measures.** Government shall implement appropriate security measures to guard against unauthorized access, unlawful disclosure of information, and to ensure the integrity of stored information.

e) **Auditability.** All systems installed shall provide for an audit trail.

Principles. The task force recognized the need to set down general guidelines or principles to aid individual government agencies with respect to their plans to comply with Section 27 of the Act, i.e., to perform their functions electronically. Perhaps the most noteworthy of the above principles is paragraph (c) on the elimination of red tape. Essentially, it was feared that without the re-examination of government processes, there is a danger of computerizing red tape and inefficient processes. Hence, paragraph (c) authorized individual government agencies to streamline their procedures to adapt to the technology and to maximize efficiency in the delivery of essential government services.

Section 39. *Government Information System Plan (GISP).* It is hereby mandated that the GISP shall be adjusted, modified and amended to conform to the provi-

sions and requirements of the Act, RPWEB and these Rules.

GISP. The GISP is the Philippine government's blueprint for introducing information technology to every aspect of its operations. For more information, please visit www.neda.gov.ph.

Chapter II - RPWEB

Section 40. *RPWEB To Promote the Use Of Electronic Documents and Electronic Data Messages In Government and to the General Public.* Within two (2) years from the effectivity of the Act, there shall be installed an electronic online network in accordance with Administrative Order 332 and House of Representatives Resolution 890, otherwise known as RPWEB, to implement Part IV of the Act 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 and to the regional and provincial offices as practicable as possible, government-owned and -controlled corporations, local government units, other public instrumentalities, universities, colleges and other schools, and universal access to the general public.

The RPWEB network shall serve as initial platform of the government information infrastructure to facilitate the electronic online transmission and conveyance of government services to evolve and improve by better technologies or kinds of electronic online wide area networks utilizing, but not limited to, fiber optic, satellite, wireless and other broadband telecommunication mediums or modes.

RPWEB. RPWEB is a strategy requiring all agencies and offices of the Philippine government to connect to the Internet. It is embodied in Administrative Order No. 332 dated November

7, 1997 (AO 332) and the above provision should be read in relation to the same. Hence, the following matters referred to in the AO are relevant:

(a) All government agencies may use their savings to purchase hardware and software necessary for Internet connection (Sec. 5, AO 332);

(b) All ISPs servicing government offices should be connected to a local Internet exchange (Sec. 3[a], AO 332); and,

(c) Telecommunications carriers should give priority to the needs of ISPs for leased lines, dial-up lines and trunking facilities (Sec. 3[b], AO 332).

Section 41. *Implementing Agencies.* To facilitate the rapid development of the government information infrastructure, the Department of Transportation and Communications, National Telecommunications Commission and the National Computer Center shall in coordination with each other, promulgate the appropriate issuances in accordance with their respective mandate to aggressively formulate, promote and implement a policy environment and regulatory or non-regulatory framework that shall lead to the substantial reduction of costs of including, but not limited to, leased lines, land, satellite and dial-up telephone access, cheap broadband and wireless accessibility by government departments, agencies, bureaus, office, government-owned and -controlled corporations, local government units, other public instrumentalities and the general public, to include the establishment of a government website portal and a domestic internet exchange system to facilitate strategic access to government and amongst agencies thereof and the general public and for the speedier flow of locally generated internet traffic within the Philippines.

Implementation. Note that the DOTC, NTC and NCC are mandated to formulate and implement, among others, a regula-

tory framework that will lead to substantial reduction of telecommunications costs not only for government but for the general public. Pursuant to this authority, the three (3) agencies are expected to issue separate implementing rules and regulations to implement Section 28 of the Act.

Section 42. Cable Television and Broadcast as Telecommunications. The physical infrastructure of cable TV and wireless systems for cable TV and broadcast excluding programming and content and the management thereof shall be considered as within the activity of telecommunications for the purpose of electronic commerce and to maximize the convergence of ICT in the installation of the government information infrastructure.

Mass Media. The Constitution provides that the ownership and management of mass media shall be limited to citizens of the Philippines, or to corporations, cooperatives or associations, wholly-owned and managed by such citizens.

For purposes of this provision (which likewise appeared in the 1973 Constitution), the Department of Justice (DOJ), citing Webster's, defined mass media "as a medium of communication (as the newspapers, radio, motion pictures, television) that is designed to reach the mass of the people and that tends to set the standards, ideals and aims of the masses" (DOJ Op. No. 163, S. 1973). In the same opinion, the DOJ likewise relied upon the definition prepared by the Media Advisory Council, to wit:

"x x x the gathering, transmission, of news, information, messages, signals and forms of written, oral and all visual communication and shall embrace the print media, radio, television, films, movies, wire and radio communications services, advertising in all its phases, and their business management" (*ibid.*).

Notably, the recording business has been expressly excluded from the Constitutional prohibition via a Presidential Memorandum signed in 1994 (Memorandum dated May 5, 1994).

Limitations. As a result of the mass media limitation, no foreign equity is allowed in broadcast or cable companies. However, convergence is expected to blur the distinction between these companies and telephone companies as they will all be enabled to carry not only images and sound but data and voice. Already, cable companies are offering high-speed Internet services or broadband over their networks. In addition, existing technologies would allow them to offer voice services. However, these developments are hampered by the Constitutional limitations on foreign ownership because it is believed that foreign investments and expertise are needed for growth in this sector.

Spin Off. In order to address this limitation, the above provision was enacted to allow either a broadcast or cable company to spin-off into two (2) companies. One will provide content and programming either in the form of licensed foreign programming or locally produced shows. This will continue to be a mass media company and subject to the Constitutional limitation against foreign ownership and management.

The other company will hold the physical infrastructure meaning in the case of broadcast companies, the broadcast equipment, licenses, and towers. This company would now be considered a telecommunications company and therefore under the Constitution, may admit up to forty percent (40%) direct foreign equity. This "physical infrastructure" company can now offer voice, data, broadband and other services provided, of course, it secures the necessary permits and licenses from Congress and the National Telecommunications Commission.

Chapter III - Delineation of Functions

Section 43. Delineation of Functions and Coordination by the DTI. In the implementation of the Act, the following government agencies shall have the functions stated hereunder:

a) The Department of Trade and Industry shall:

(i) Supervise and coordinate the full implementation of Section 27 of the Act. For this purpose, all government agencies intending to comply with the said provision of law shall coordinate with the DTI in order to ensure adherence with the principles provided for in Section 38 of these Rules. Observance of all laws and regulations on public bidding, disbursements and other restrictions, including COA policies, shall be mandatory.

(ii) Install an online public information and quality and price monitoring system for goods and services aimed in protecting the interests of the consuming public availing of the advantages of the Act.

(iii) Establish a voluntary listing system for all businesses or entities involved in electronic commerce including, but not limited to, value-added service (VAS) providers as this term is understood in Republic Act No. 7925, banks, financial institutions, manufacturing companies, retailers, wholesalers, and on-line exchanges. The list of electronic commerce entities shall be maintained by the DTI and made available electronically to all interested parties.

(iv) Review, study and assess all legal, technical and commercial issues arising in the field of electronic commerce which may be directed to the DTI and if necessary, convene the appropriate government agencies in order to discuss, deliberate on and resolve the same and in the proper cases, promulgate additional rules and regulations to implement the Act.

b) The Bangko Sentral ng Pilipinas shall exercise and perform such functions as mandated under the Act including the promulgation of the rules and regula-

tions to implement the provisions of the Act with respect to banks, quasi-banks, trust entities, and other institutions which under special laws are subject to the Bangko Sentral ng Pilipinas supervision

c) The Department of Budget and Management shall identify the fund source for the implementation of Sections 37, 39 and 40 of the Rules, consistent with the provisions of the annual General Appropriations Act, and in its capacity in managing the budget execution and accountability processes of government, shall be responsible for putting such core processes online.

Delineation of Functions. As mandated, each and every agency of the government is tasked with the implementation of the Act in accordance with their respective areas of authority. In other words, the Bangko Sentral Ng Pilipinas will regulate electronic banking while the Securities and Exchange Commission will issue the rules on electronic stock trading and virtual stock exchanges.

Implementation of Section 27. The Department of Trade and Industry ("DTI") however is tasked with coordinating the implementation of Section 27 of the Act respecting the mandate to government to conduct its business electronically. In this regard, DTI will monitor the progress by individual government agencies and ensure compliance with the principles set forth in Section 38 of the IRR.

One Stop Shop. Section 43(a)(iv) was included in the IRR in order to address concerns relating to electronic commerce where the party is unsure which government agency to approach. In such cases, the party can go to the DTI which will take the appropriate action regarding such concerns. For its part, the DTI is currently studying the establishment of a One Stop Shop or help desk to perform this function and address these issues.

Voluntary List. As part of DTI's efforts to promote elec-

tronic commerce, it will host a list of companies engaged in electronic commerce. Registration in the list is purely voluntary.

PART V

FINAL PROVISIONS

Section 44. *Extent of Liability of a Service Provider.* Except as otherwise provided in this Section, no person or party shall be subject to any civil or criminal liability in respect of the electronic data message or electronic document for which the person or party acting as a service provider as defined in Section 6(n) of these Rules merely provides access if such liability is founded on:

a) The obligations and liabilities of the parties under the electronic data message or electronic document;

b) The making, publication, dissemination or distribution of such material or any statement made in such material, including possible infringement of any right subsisting in or in relation to such material: **Provided, That**

(i) The service provider: (1) does not have actual knowledge, or (2) is not aware of the facts or circumstances from which it is apparent, that the making, publication, dissemination or distribution of such material is unlawful or infringes any rights subsisting in or in relation to such material, or (3) having become aware, advises the affected parties within a reasonable time, to refer the matter to the appropriate authority or, at the option of the parties, to avail of alternative modes of dispute resolution;

(ii) The service provider does not knowingly receive a financial benefit directly attributable to the unlawful or infringing activity; and,

(iii) The service provider does not directly commit any infringement or other unlawful act and does not induce or cause another person or party to commit any infringement or other unlawful act and/or does not benefit financially from the infringing activity or un-

lawful act of another person or party;

Provided, further, That nothing in this Section shall affect-

a) Any obligation founded on contract;

b) The obligation of a service provider as such under a licensing or other regulatory regime established under written law;

c) Any obligation imposed under any written law; or,

d) The civil liability of any party to the extent that such liability forms the basis for injunctive relief issued by a court under any law requiring that the service provider take or refrain from actions necessary to remove, block or deny access to any material, or to preserve evidence of a violation of law.

Source. This provision is based on Section 10 of the ETA and §512(c)(1) of the U.S. Digital Millennium Copyright Act of 1998 ("DMCA"). This provision did not appear from SB 1902 but was carried over because of HB 9971. At the Senate, it was removed when Sen. Raul Roco suggested a return to the UNCITRAL Model Law framework.

Basis. The above-provision is the codification of jurisprudence in other countries, notably, the United States. In *Cubby v. Compuserve*, (776 F.Supp 135 [SDNY 1991]), it was held that Compuserve's lack of editorial control over content located within its servers absolved it from liability for defamation. The court in that case determined that Compuserve was a mere distributor of information and was no more liable for defamation than a bookseller or library would with respect to the books found therein. In contrast, the Supreme Court of New York in *Stratton Oakmont, Inc. v. Prodigy Services Co.* (23 Media L. Rep. [BNA] ¶ 1794, 1995 N.Y. Misc. LEXIS 229, 1995 WL 323710 [N.Y. Sup. Ct. May 24, 1995]), held Prodigy liable as a publisher because it held itself out as controlling the content of its bulletin boards. Editorial control there-

fore was critical in determining a service provider's liability for content.

In the realm of copyright, the District Court of the Hague held in *Church of Scientology v. Dataweb et al.*, (Cause No. 96/1048 [Dist. Ct. of the Hague, Holland, June 9, 1999]) that Internet Service Providers could not be held liable for infringement because their activities are limited to providing information from and/or to its users and the storage of this information. In addition, the service providers do not select the information and do not process it either. They only provide the technical means to enable publication by others. Hence, in these circumstances the service providers do not do the publishing themselves, but only provide the opportunity for publication.

Liability. The liability of the service provider herein is limited not only to that arising from copyright infringement but to a whole range of offenses against third parties. It includes libel, defamation, threats, pornography, as well as, the illegal conduct of its clients.

During the Senate interpellation of SB 1523 (later SB 1902), Sen. Gregorio Honasan inquired if service providers should be held liable for pirated or infringing material even though they are unaware of the same. Sen. Magsaysay expressed the opinion that absent any active involvement by the service provider, it should not be liable for piracy or infringement. If the law were to provide otherwise, service providers would be constrained to monitor all electronic traffic in order to avoid suit. This, of course, might constitute an invasion of privacy and result in other unintended harms.

Modification in the IRR. Subsection (3) in subparagraph (b)(i) was introduced to the IRR by the task force. The original provision appearing as Section 30(b)(i) of the Act imposed liability upon the service provider when it becomes aware of the infringement

or unlawful violation of the rights of a third party. It was believed, however, that if the provision were to remain unchanged or modified, it may be used to work an injustice against persons with legitimate rights.

For example, if A's website is hosted by service provider X and the latter receives notice from B that A's site contains infringing material (something which is untrue), X would be forced to take down or remove A's site based on B's notice. This is due largely to the fact that under the Act, once the service provider X becomes aware of an infringement, it may become liable therefor. Consider for the moment the fact that B's notice was incorrect – A was *not* committing infringement. Yet despite such false information, A's site was taken down and the latter suffers the consequences thereof.

It was suggested that the IRR instead adopt the "notice and take down" provision appearing in the DMCA. Under §512(c)(1) of the DMCA, a service provider, in order to avoid liability, must remove the infringing material after it has received an infringement notice. In order to avoid or minimize the injustice referred to in the preceding paragraph, the DMCA mandates that the infringement notice be made under penalty of perjury, among other requirements.

The task force was of the opinion however that the protection under the DMCA might be ineffective in the Philippine setting since the threat of perjury is not enough of a deterrent against false infringement notices. While perjury is a criminal offense under Philippine law, there is a perception that it is not adequately enforced.

Hence, the rule was adopted which gives the service provider the opportunity to refer the matter and the parties to the proper government agency or to arbitration. After receiving an infringement notice, the service provider need not take any ad-

verse action against any party and instead gives the parties the full opportunity to ventilate their dispute before the proper forum.

Lawful Access

Section 45. Lawful Access to Electronic Documents, Electronic Data Messages, and Electronic Signatures. Access to an electronic file, or an electronic signature of an electronic data message or electronic document shall only be authorized and enforced in favor of the individual or entity having a legal right to the possession or the use of the plaintext, electronic signature or file and solely for the authorized purposes.

Source. The above was inspired by the ETA provisions authorizing the government to conduct investigations requiring access to computers and data.

Lawful Access. Apart from persons authorized by the individual having possession of the electronic document or signature, the appropriate government agency or entity (including police officers) may have access to the same provided they comply with the Constitutional protection against unreasonable searches and seizures (Section 2, Article III, Constitution). Law enforcement agencies must therefore procure a search warrant before conducting a search of a computer containing electronic evidence.

Lawful Search. A number of issues will arise once search warrants are issued respecting electronic signatures and documents. The Constitution provides, among others, that the search warrant must particularly describe "the place to be searched and the persons or things to be seized." In the context of a computer, this may be interpreted to mean that the search is limited only to a particular folder or sub-directory. If so, questions will arise if the law enforcement officer can seize the entire computer – CPU, Monitor and all. A seizure of that

nature may be considered beyond the bounds allowed by the Constitution.

Other novel issues are likely to arise relating to established doctrine such as that upholding plain view searches. Under that doctrine, so long as the law officer has a right to the view, if he detects contraband that item may be seized and the possessor charged appropriately. This is true despite the fact that the item was not specified in the search warrant. The rule likewise applies in instances where there is no search warrant at all – so long as the officer has a right to the view, it would be a valid search. Applying the rule to computer searches, a law officer may, for example, have a search warrant for a particular file but in the course of the computer search, he discovers a pirated copy of a software application. In such cases, the plain view search rule may be used to justify charging the owner of the computer with copyright infringement. On the other hand, the search may be considered illegal and the application of the rule assailed.

It is therefore suggested that the Department of Justice issue guidelines regarding the search and seizure of computers and computer files. In this regard, they can examine similar rules issued by the U.S. Department of Justice.

Criminal Liability. Section 33(d) of the Act (Section 51 of the IRR) penalizes “other violations of the provisions” of the Act with a fine or imprisonment. It may be said therefore that the failure to comply with this provision and Sections 46 and 47 of the IRR constitutes a criminal offense under the Act.

Section 46. Lawful Access to Electronic Keys. The electronic key for identity or integrity shall not be made available to any person or party without the consent of the individual or entity in lawful possession of that electronic key. The testimonial disclosure of an elec-

tronic key in any proceeding shall be limited by the Constitutional right against self-incrimination.

Self-incrimination. The last sentence of the provision was added into the IRR to address the situation where law enforcement officers in the course of investigation compel witnesses to disclose their encryption keys. It is expected that much of the information contained in computers will be encrypted. It is therefore important to establish that the right against self-incrimination can be used by the person under investigation to resist the compulsion to disclose the electronic key. The only other alternative to law enforcement agencies is to use “brute force” to decrypt the information. (i.e., use every possible key until finding one that works; depending upon the computer used, this process may take weeks or even years for power encryption).

Section 47. Obligation of Confidentiality. Except for the purposes authorized under the Act, any person who obtained access to any electronic key, electronic data message, or electronic document, book, register, correspondence, information, or other material pursuant to any powers conferred under the Act, shall not convey to or share the same with any other person.

Source. This is based upon Section 48 of the ETA.

Application. This provision is also addressed to law enforcement officers who, through the service of search warrants, come into the possession or acquire access to electronic keys and evidence. It may be said that the violation of this obligation is a criminal offense under Section 33(d) of the Act.

Penal Provisions

Section 48. Hacking. 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.

Love Bug. This provision gained media attention before the Act was signed into law because of the I Love You Virus incident. It was alleged that a Filipino created and released the virus, nicknamed the Love Bug. However, the absence of any law on the subject of viruses caused the dismissal of the all criminal actions filed by the National Bureau of Investigation (“NBI”) with the Department of Justice.

It was observed that had the Act been passed before the Love Bug incident, then its provisions penalizing the release of viruses could have been used to charge the accused. Additionally, it would have allowed the United States to request the extradition of the suspect. The absence of any criminal liability for such things as hacking raised concerns that the Philippines would be a safe harbor for cybercriminals. As a result of the Love Bug incident, public attention over the passage of the law was heightened and hastened the passage of the Act.

Hacking. Note that various acts are punished under the law and these may be categorized as follows:

- (a) **Unauthorized access** into a computer system;
- (b) **Interference** in a computer system/server or informa-

tion and communication system;

(c) Authorized access in order to corrupt, alter, steal, or destroy without the knowledge and consent of the owner of the computer or information and communications system; and,

(d) The introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document

Note that all types of unauthorized access will constitute hacking while only certain types of authorized access will be punishable. For authorized access to rise to the crime of hacking it must be done “in order to corrupt, alter, steal, or destroy” data. The destruction or corruption of data through authorized access say, by disgruntled employees will likewise constitute hacking. Proving the “stealing” or theft of data may prove difficult because unlike tangible objects, when data is stolen, it remains in the possession of its owner – but the thief likewise obtains possession.

Interference with a computer system includes the Distributed Denial of Service (DDoS) Attacks which crippled well-known sites such as eBay, Yahoo!, Amazon and CNN.

In addition, while the release of viruses is punished, it seems that the perpetrator is not separately liable for the subsequent transmission or spread of the virus. This is in contrast with the Computer Fraud and Abuse Act of the United States where a person who knowingly causes the transmission of the virus is criminally liable (U.S.C. Title 18 §1030[a][5][A]) for every instance of infection.

Finally, it should be noted that the crime of hacking may occur even if the computer system is a stand-alone machine which is not part of a network or even connected to the Internet. Hence, if a word processing file is password-protected and a person defeats the password without the consent of the owner,

it would constitute hacking.

Penalty. The penalty for hacking includes a mandatory imprisonment. Hence, even though the term of imprisonment would otherwise have qualified the convict to apply for probation, the same would be disallowed.

In addition, note that there is no ceiling for the fine that will be imposed. If the Love Bug incident had occurred after the Act had been passed, the convict would presumably have paid a fine equal to US\$9 billion – the total worldwide damage wrought by the virus. It is submitted that under these circumstances the penalty may be declared unconstitutional for being a cruel and unusual punishment.

Section 49. Piracy. 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. The foregoing shall be without prejudice to the rights, liabilities and remedies under Republic Act No. 8293 or Intellectual Property Code of the Philippines and other applicable laws.

Piracy. This is a new form of piracy which is done through the use of “telecommunication networks” such as the Internet. It remains to be seen however, if a local area network (LAN) or some other private network will be considered a “telecommuni-

cation network” for purposes of this provision.

The provision also covers all types of intellectual property rights including patents and trademarks. It is not inconceivable for one to interpret this provision as being applicable to a case of cybersquatting of a registered trademark. The plaintiff-trademark holder may claim that the registration of the domain name constitutes an unauthorized “use.”

The Intellectual Property Office suggested the addition of the final sentence to clarify that the criminal liability under the Act is separate and independent from the criminal liability under the Intellectual Property Code.

Section 50. Other Penal Offenses. Violations of the Consumer Act or Republic Act No. 7394 and other relevant or pertinent laws through transactions covered by or using electronic data messages or electronic documents, shall be penalized with the same penalties as provided in those laws.

Rationale. This was added in order to explicitly provide for the application of the Act to existing law. The special reference to the Consumer Act was prompted by concerns from various sectors relating to the protection afforded to Filipino consumers transacting over the Internet.

In particular, Sen. Gregorio Honasan asked during the Senate interpellation of SB 1523 (later SB 1902) if online buyers were clearly protected by law. In response, Sen. Magsaysay answered that the Act would, at the very least, provide assurance to aggrieved parties that their electronic evidence of the transaction would be admissible in court. But admissibility is to be distinguished from the weight and sufficiency of the electronic evidence which is addressed to the sound discretion of the court.

Section 51. *Other Violations of the Act.* Other violations of the provisions of the Act, shall be penalized with a maximum penalty of one million pesos (P1,000,000.00) or six-(6) years imprisonment.

Miscellaneous Provisions

Section 52. *Statutory Interpretation.* Unless otherwise expressly provided for, the interpretation of these Rules and the Act shall give due regard to the Act's international origin - the UNCITRAL Model Law on Electronic Commerce - 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.

Section 53. *Variation by Agreement.* - Any provision of the Act may be varied by agreement between and among parties; Provided that such agreement involves only the generation, sending, receiving, storing or otherwise processing of an electronic data message or electronic document. Nothing shall authorize contracting parties to agree upon stipulations or covenants, which defeat the legal recognition, validity and admissibility of electronic data messages, electronic documents, or electronic signatures.

Source. This provision was based on Article 4 of the Model Law. Notably, that provision limited the right to vary the Model Law only to matters relating to electronic contracts, attribution of data messages, acknowledgement of receipt, and time and place of dispatch and receipt of data messages.

Scope. Section 38 of the Act implies that any provision thereof may be varied by the agreement of the parties. This was identified by the task force as a potential problem because a blanket authority to vary the terms of the Act would enable parties

to agree, for example, that with respect to their transaction, no electronic document or signature would be valid or admissible. In other words, Section 38 seemed to give contracting parties the wholesale right to defeat the expressed provisions of the Act.

After consulting with members of the technical working group of the Bicameral Conference Committee, it was explained that an agreement to vary the terms of the Act may only involve the generation, sending, receiving, storing or otherwise processing of an electronic data message or electronic document. This interpretation is parallel to the provision in the Model Law. But to stress the point further, the final sentence was added into the IRR to clarify that nothing in the Act authorizes anyone to defeat the legal recognition of electronic documents and signatures.

Section 54. *Reciprocity.* All benefits, privileges, advantages or statutory rules established under this Act, including those involving practice of profession, shall be enjoyed only by parties whose country of origin grants the same benefits and privileges or advantages to Filipino citizens. Inasmuch as the Act merely contemplates the legal recognition of electronic forms of documents and signatures and does not amend any law governing the underlying substantive validity of acts or transactions, this provision shall be subject to existing Constitutional and statutory restrictions relative to activities which are reserved to Philippine citizens or juridical entities partially or wholly-owned by Philippine citizens.

Section 55. *Oversight Committee.* There shall be a Congressional Oversight Committee composed of the Committees on Trade and Industry/Commerce, Science and Technology, Finance and Appropriations of both the Senate and House of Representatives, which shall meet at least every quarter of the first two years and every semester for the third year after the

approval of this Act to oversee its implementation. The DTI, DBM, Bangko Sentral ng Pilipinas, and other government agencies as may be determined by the Congressional Committee shall provide a quarterly performance report of their actions taken in the implementation of this Act for the first three (3) years.

Source. This provision was suggested by Rep. Verceles to ensure the proper implementation of the Act particularly Section 27 (on the government recognition of electronic documents).

Section 56. *DTI's Continuing Authority to Implement the Act and Issue Implementing Rules.* Among others, the DTI is empowered to promulgate rules and regulations, as well as provide quality standards or issue certifications, as the case may be, and perform such other functions as may be necessary for the implementation of this Act in the area of electronic commerce.

Section 57. *Separability.* If any provision in these Rules or application of such provision to any circumstance is held invalid, the remainder of these Rules shall not be affected thereby.



This project was assisted by

**THE TRADE AND INVESTMENT POLICY ANALYSIS
AND ADVOCACY SUPPORT PROJECT**

a project of the Philippine Exporters Confederation, Inc. in cooperation with the United States Agency for International Development. The TAPS Project supports the improvement of the policy and regulatory environment which impact on productive investment and trade.