When life and liberty are at stake, the Supreme Court should not abuse its rule-making power to the disadvantage of the accused. No court is more supreme than the fundamental law and as former Supreme Court Justice Claudio Teehankee Jr. once said, the rule of law shall always prevail.

communicate with counsel of defendant's choosing; the right to free legal assistance for defendants unable to pay for it; the right to examine witnesses for the prosecution and to present witnesses for the defence; the right to free assistance of an interpreter if the defendant cannot understand or speak the language of the court.

The Digital Trail: Picking Up Hansel and Gretel's Breadcrumbs and Presenting Them in Court

Anna Maria Karla B. Ng★

I. INTRODUCTION

Computers now create, store, retrieve, and reproduce a large amount of information in the country. Offices use computers to perform a multitude of tasks ranging from the clerical to the consequential in the course of their transactions and conclusion of their contracts. With technology ingrained as an accepted manner of conducting business, electronically generated information plays an increasingly important role in the lives of individuals coming under Philippine jurisdiction. Thus, it is incumbent upon legal practitioners to recognize this regular, albeit new, manner of business.

★ '06 J.D. cand., Ateneo de Manila University School of Law; Member, Executive Committee, *Ateneo Law Journal*. Her previous works published in the *Journal* include: *The Talents of a Talent:* Sonza v. ABS-CBN Broadcasting Corporation, 49 ATENEO L.J. 837 (2004); *Citizenship: Man's Being Defined and Undefined in Light of* Tecson et. al. v. COMELEC, 49 ATENEO L.J. 291 (2004); In Re Purisima: *Competence and Character Requirement for Membership in the Bar,* 48 ATENEO L.J. 840 (2003) with Ms. Aimee Dabu et al.

Cite as 50 ATENEO L.J. 175 (2005).

The legislature has responded with the enactment of laws that recognize the need for laws pertinent to the use of electronics. First, the Electronic Commerce Act[1] requires the signature of electronic legal documents in order that commercial transactions may be conducted in electronic form, and criminalizes two major cyber-crimes – computer hacking and piracy.[2] Second, the Consumer Act[3] provides that violations thereof, if performed through electronic data messages or electronic documents, shall be punished accordingly by express mandate of the Electronic Commerce Act.[4] Third, the Optical Media Act[5] calls for the protection and promotion of intellectual property rights through the regulation of the manufacture, mastering, replication, importation, and exportation of optical media. Fourth, the Access Devices Regulation Act of 1998[6] seeks to protect the rights and define the liabilities of parties in commercial transactions using access devices by regulating the issuance and use of such devices.

In addition, there are four Anti-Cyber Crime bills pending with the House of Representatives. House Bill Nos. 1246, 2093, 2528, and 3777 provide coverage on activities ranging from computer fraud, computer forgery, unauthorized computer access to data authentication, and secure online commercial transaction.

House Bill No. 1246 "seeks to protect and safeguard the integrity of computers, computer systems, computer networks, computer servers, database, and information and data stores from computer users who resort to computer fraud, abuses, and other cyber-related fraudulent activities, by providing penal sanctions to the perpetrators."[7] It calls for the creation of a

1. An Act Providing for the Recognition and Use of Electronic Commercial and Non-Commercial Transactions and Documents, Penalties for Unlawful Use Thereof and for other Purposes, Republic Act No. 8792, [ELECTRONIC COMMERCE ACT OF 2000].
2. *Id.*
3. The Consumer Act of the Philippines, Republic Act No. 7394 (1992) [CONSUMER ACT].
4. ELECTRONIC COMMERCE ACT OF 2000, § 33 (c).
5. An Act Regulating Optical Media, Reorganizing for this Purpose, the Videogram Regulatory Board, Providing Penalties Therefore, and for Other Purposes, Republic Act No. 9239, (2004) [OPTICAL MEDIA ACT].
6. An Act Regulating the Issuance and Use of Access Devices, Prohibiting Fraudulent Acts Committed Relative Thereto, Providing Penalties and for Other Purposes, Republic Act No. 8484, (1998) [ACCESS DEVICES REGULATION ACT OF 1998].
7. An Act Preventing and Penalizing Computer Fraud, Abuses and Other Cyber-related Fraudulent Activities, and Creating for the Purpose the Cyber-crime Investigation and Coordinating Center, Prescribing its Powers and Functions, and Appropriating Funds Therefore, House Bill No. 1246, 13TH Cong. (2004) [ANTI-CYBER CRIME ACT OF 2001].

coordinating body, the Cyber-Crime Investigation and Coordinating Center (CICC), which shall "coordinate, collate and synergize efforts of all law enforcement agencies in combating cyber crimes."[8]

House Bill No. 3777 "seeks to define cybercrime, identify punishable acts involving computers, provide penalties, determine legal procedures for the investigation and prosecution of cybercrimes, clarify jurisdiction and provide for a clause on mutual assistance and cooperation."[9]

There is also a pending bill which seeks to merge the communications aspect of the Department of Transportation and Communications (DOTC) with the National Computer Center (NCC), which is presently under the Office of the President (OP), with the purpose of streamlining its inherent functions to address the new phenomenon of converging and emerging information technologies; it shall become the Department of Information and Communications Technology.[10]

In line with this, President Arroyo issued Executive Order No. 269 last January which created the Commission on Information and Communications Technology (CICT). Director Rica Adriatico of the Department of Budget and Management (DBM) reported that the DBM has released a total of P1.3 billion for information and communications technology projects.[11]

These technology projects will be pivotal in advancing the computer forensics capabilities of the government. As of today, there are only two government offices that are capable of performing computer forensics operations.[12] The first is the National Bureau of Investigation (NBI)

8. *Id.* in Abstract.
9. An Act Defining Cybercrime, Providing for Prevention, Suppression and Imposition of Penalties Therefor and for other Purposes [CYBERCRIME PREVENTION ACT OF 2005], House Bill No. 3777, 13TH Cong. (2005).
10. An Act Creating The Department Of Information And Communications Technology, Defining Its Powers And Functions, Appropriating Funds Therefor And For Other Purposes, House Bill No. 557, 13TH Cong. (2004) [DEPARTMENT OF INFORMATION AND COMMUNICATIONS TECHNOLOGY ACT OF 2004].
11. *DBM Funds IT Projects*, House of Representatives Website, *available at* http://www.congress.gov.ph/committees/commnews/commnews_det.php?newsid= 166&key=information (last accessed August 24, 2005).
12. Interview with Atty. Geronimo L. Sy, State Prosecutor, Department of Justice, in Makati, Metro Manila (August 22, 2005).

through its Anti-Fraud Department. The second is the Criminal Investigation & Detection Group (CIDG) of the Philippine National Police (PNP). In fact, after an investigation in collaboration with Department of Justice, through State Prosecutor Geronimo L. Sy, Manila Regional Trial Court Judge Antonio Eugenio ordered the arrest of "JJ Maria Giner," a Filipino hacker believed responsible for the hacking of the government portal "gov.ph."[13] Sufficient evidence has been gathered to convict him under section 33(a) of the E-Commerce Act.[14]

The creation of the Department of Information and Communications Technology will definitely be advantageous and beneficial for the integration of computer forensics in the country. Furthermore, it becomes crucial that new policies are implemented which deal with the growing sophistication of cyber-crimes in the country. Getting tough on illegal computer activities committed in cyberspace and within the Philippine jurisdiction and creating new laws to govern technology and safeguard citizens will undoubtedly improve our country's competitive position in the global market.

For its part, the Supreme Court issued a circular, the Rules on Electronic Evidence.[15] Most individuals presume that these rules apply to civil actions and proceedings and to quasi-judicial and administrative cases only, but the Supreme Court issued another resolution that states that the same rules shall be applicable to criminal actions and proceedings, in addition to those previously mentioned.[16] Despite this, there is still little use for electronic evidence in court, and the number of Supreme Court cases that deal with the same are few.[17]

13. Court Orders Arrest of Suspected Government Website Hacker, *available at* http://asianjournal.com/cgi-bin/view_info.cgi?code=00009122&category (last accessed August 22, 2005).

14. Interview with Atty. Geronimo L. Sy, State Prosecutor, Department of Justice, in Makati, Metro Manila (August 22, 2005).

15. A.M. NO. 01-7-01-SC, effective August 1, 2001.

16. Amendment to A. M. No. 01-7-01-SC, effective October 14, 2002.

17. *See* People v. Burgos, 200 SCRA 67 (1991) (Printing of files from a diskette was disallowed by the trial court because of its vulnerability to manipulation, but should have been allowed, as opined by the Supreme Court); Metropolitan Bank and Trust Company v. NLRC, 235 SCRA 400 (1994); IBM Philippines v. NLRC, 305 SCRA 592 (1999) (Warnings of impending disciplinary action regarding tardiness and absenteeism were sent to an employee through the company's e-mail system were held as inadmissible for not being properly signed and identified); People v. Ordoño, 334 SCRA 673 (2000) (Interview recorded by an electronic device held as admissible because it was properly presented in court); People v. Williams, 357 SCRA 124 (2001) (Passenger manifest is considered hearsay and therefore inadmissible without the accompanying testimony of the employee who recorded the seat number); Nuez v. Apao, 455 SCRA 288 (2005) (Text messages were held admissible to prove that respondent sought PIM from complainant in exchange for favorable decision in a Court of Appeals case in which the former was interested).

The advocates of the Philippine legal system, however, have become more inclined to use electronic information and devices in the practice and examination of the law. For example, the Supreme Court has devised a five year plan from 2003 to 2007 called the *Information System Strategic Plan,* which includes the Library Information Management System (LIMS) and the Legal Research System (LRS).[18] These two portions of the plan enable researchers "through a computer-based system that allows browsing through an electronic compilation of full text of Supreme Court decisions.... to search for a jurisprudence or decision related to or pertaining to a particular subject using search delimiters."[19] Likewise, mobile phones are becoming relevant as (computer) forensic evidence in trials.[20] For instance, a satellite triangulation technique called "cell site analysis" can provide forensic evidence to determine the location of a mobile phone when it is used.[21]

Meanwhile, in the United States the enactment of the Sarbanes-Oxley Act of 2002[22] requires the preservation of potential evidence, including electronic evidence, and calls for corresponding penalties for destruction of records. As a response to highly publicized cases of corporate fraud in the United States, the Sarbanes-Oxley Act helps investigators and legal practitioners build cases against violators who fail to retain e-mails, electronic files, and other relevant data. Also in the United States, the Patriot Act,[23] enacted in response to the events of September 11, 2001, allowed law enforcement agencies to obtain information from Internet Service Providers (ISPs) without the need of a warrant due to the Act's "threat to life and limb" provision.[24] Violation of civil liberties aside, the responsiveness of the

18. ALFREDO S. VITANGCOL III, TECHNOLAWGY: A LAWYER'S GUIDE TO INFORMATION TECHNOLOGY IN THE PRACTICE OF LAW 27 (2004).

19. *Id.*

20. *See Trial and Triangulation*, THE ECONOMIST, December 18, 2003.

21. *Id.*

22. Sarbanes-Oxley Act of 2002, *available at* http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf (last accessed Sept. 07, 2005).

23. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, [USA Patriot Act] Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001).

24. *See* EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME 10 (2d ed. 2004).

United States government to the rise of digital information is strengthened because of the Patriot Act.

While it is definitely good news that the legal system adapts to technological advancements, it remains unclear how these advancements can improve the dispensation of justice throughout society. Integration of technology should not be the only goal; rather, making the most out of what technology offers and streamlining these benefits to fit the existing legal system should be the main focus.

The use of electronic devices and the extent of discovery which can be made from them will be explored in this Note in light of existing rules and jurisprudence relating to the presentation of electronic evidence.

II. SURVEY OF LAWS

Currently, there are few laws that specifically and exclusively govern electronic devices and other issues related thereto, such as prosecution of crimes arising from their use and the regulation thereof. A number of statutes make reference to the same. According to a McConnell international study, the Philippines was included in the list of the 53 nations that had the ability to prosecute computer crimes in the year 2000.[25] But the state of laws leaves much to be desired because some provisions are ambiguous, too technical, or worse, simply non-existent. In the same year, but shortly before the passage of the E-Commerce Act, investigations of the ILOVEYOU virus alleged that a Filipino student, Onel de Guzman, was responsible for its creation.[26] However, the "lack of a law that specifically addressed the situation hampered attempts at prosecution."[27] The virus reportedly amounted to a global damage of seven billion U.S. dollars.[28] The gravity of the damage and international scrutiny led to efforts to immediately produce the E-Commerce Act, which punishes three types of offenses.[29] The first offense is unauthorized access to a computer system; the second offense is piracy; and

25. TECHNOLAWGY, *supra* note 18, at 68.

26. The ILOVEYOU virus came in the form of an e-mail attachment, which, if opened, re-sent itself to all the addresses in the first recipient's address book and caused the loss of numerous files on the recipient's hard disk. MELYJANE BERTILLO, HANNIBAL BOBIS & MILABEL MUJER, ET. AL., CYBERCRIME: THE NEED FOR NEW LEGISLATION IN THE PHILIPPINES (2002).

27. *Id.* at 10.

28. *Id.* at 18, *citing* George Urbass, *Cybercrime Legislation in the Asia Pacific Region, available at* www.aic.gov.au (last accessed Sept. 07, 2005).

29. ELECTRONIC COMMERCE ACT OF 2000, § 33.

the third refers to violations of the Consumer Act "through transactions covered by or using electronic data messages or electronic documents."[30]

Pursuant to a memorandum dated 18 June 2001, which was submitted to the Supreme Court by the Committee on Revision on the Rules of Court and whose objective is to reflect the changes on the rules on evidence brought about by the E-Commerce Act, the Supreme Court issued the Rules on Electronic Evidence.[31] Meanwhile, the Cyber-Crime bill, which seeks to criminalize and punish seven acts in relation to child pornography, is pending in Congress.[32]

As intimated earlier, there are other statutes that can be linked to electronic evidence. One statute is the Optical Media Act, which aims to regulate the manufacture, mastering, replication, importation and exportation of optical media.[33] Another is the Access Devices Regulation Act, which aims to "regulate the issuance and use of access devices."[34] As defined therein, "access devices" refer to:

> any card, plate, code, account number, electronic serial number, personal identification number, or other telecommunications service, equipment, or instrumental identifier, or other means of account access that can be used to obtain money, good, services, or any other thing of value or to initiate a transfer of funds (other than a transfer originated solely by paper instrument).[35]

A. The E-Commerce Act

The E-Commerce Act of 2000 was a consolidation of Senate Bill No. 1902 and House Bill No. 9971,[36] and was signed into law on June 14, 2000.[37] The bold objective of the E-Commerce Act is to promote and protect electronic commerce transactions through the adoption of an E-government

30. *Id.*

31. RULES ON ELECTRONIC EVIDENCE, A.M. No. 01-7-01-SC, effective August 1, 2001.

32. *Supra* note 7. The bill defines Child Pornography as (a) a minor engaged in sexually explicit conduct; or (b) a person appearing to be a minor engaged in sexually explicit conduct.

33. OPTICAL MEDIA ACT, § 2.

34. ACCESS DEVICES REGULATION ACT OF 1998, §22.

35. *Id.* §3 (a).

36. Ramon B. Magsaysay, Jr., *An Overview of the E-Commerce Act of 2000*, 45 ATENEO L.J. 377 (2001) (Former Senator Ramon B. Magsaysay Jr. is the author of Senate Bill No. 1902).

37. TECHNOLAWGY, *supra* note 18, at 68.

policy.[38] The E-Commerce Act does not seek to replace existing legal arrangements governing commerce, but merely to move the country to the next logical step after paper documents.[39]

Prior to the enactment of the said law, the country suffered from lack of a clearly defined e-commerce policy, and due to the absence of e-commerce legislation, Philippine businesses were limited to activities involving only purchase orders and reporting forms.[40] However, lawmakers acknowledged that Philippine businesses need to engage in e-commerce through the Internet in order to compete in the global marketplace.[41] Thus, the E-Commerce Act was passed in the hopes of triggering the development of application of online business transactions in the country.[42] This law also mandates government agencies to formally recognize the rules and regulations in furtherance of the original goals of the Act itself.[43]

The E-Commerce Act attempts to balance two interests, namely the convenience that electronic commerce provides as well as the challenges and issues that electronic commerce presents to the Philippine Rules on Evidence with respect to juridical ties between parties who contract through electronic media.[44]

This law has adopted the *functional equivalent approach* in treating documents.[45] It provides that for evidentiary purposes an electronic document shall be the functional equivalent of a written document under existing laws.[46] Electronic documents shall also have the same legal effect, validity, or enforceability provided that the same is authenticated, and the integrity and reliability of electronic documents are maintained.[47] In close connection with the functional equivalent rule is the *non-discrimination rule*. The E-Commerce Act does not automatically make an electronic document legally effective, valid, and enforceable. What it merely does is to prohibit

38. Magsaysay, Jr., *supra* note 36, at 378.

39. *Id.* at 390.

40. *Id.* at 382.

41. *Id.*

42. *Id.* at 383.

43. *Id.* at 388.

44. *Id.* at 378.

45. Francisco Ed. Lim, *Litigation in E-Commerce: Proving a Case with Electronic Documents*, 45 ATENEO L. J. 355 (2001).

46. ELECTRONIC COMMERCE ACT OF 2000, § 7, last ¶. (emphasis supplied).

47. *Id.* § 7, ¶ 1 (a).

discrimination against electronic documents as opposed to traditional paper documents.[48] The E-Commerce Act provides:

> *Sec. 12. Admissibility and Evidential Weight of Electronic Data Message and Electronic Documents.* - 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 and electronic data message or electronic document meeting, and complying with the requirements under Sections 6 or 7 hereof shall be the best evidence of the agreement and transaction contained therein.

1. Electronic Documents

Electronic documents refer 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.[49]

Just like any other documentary evidence, electronic documents must be relevant[50] and competent.[51] In addition, the E-Commerce Act provides for rules in the authentication of electronic documents. Section 11 thereof provides that an electronic data message or an electronic document shall be authenticated by proof of an *appropriate security procedure*.[52] This proof must show that the said procedure, when applicable, was adopted for the purpose of the following:

1. Verifying the originator of an electronic data message and/or electronic document; or
2. 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,

48. Lim, *supra* note 45, at 359.

49. ELECTRONIC COMMERCE ACT OF 2000, § 5 (f).

50. 1997 Revised Rules of Court, Rule 128, § 4.

51. *Id.* § 3.

52. *Id.* (emphasis supplied).

> identifying words or numbers, encryptions, answers back or acknowledgement procedures, or similar security devices.[53]

The E-Commerce Act shows liberality since evidence of the integrity of the information and communication system used may be introduced in the absence of evidence to the contrary.[54]

In case what is required is the original form of the information, the following requirements must be met:

1. Integrity to be shown by evidence *aliunde* or otherwise;[55] and
2. Proof of capability of being displayed, if information is required to be presented.[56]

2. Electronic Signatures

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.[57] The E-Commerce Act does not make mention of digital signatures unlike the Rules on Electronic Evidence which specifically includes digital signatures among *electronic signatures*.

Unlike the authentication of electronic documents that requires proof of appropriate security procedure alone, authentication of electronic signatures is done by proving either of two things:

1. 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
2. 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

53. *Id.*
54. *Id.* § 11, ¶ 2.
55. *Id.* § 10, 1(a).
56. *Id*, § 10, 1(b).
57. *Id.* § 5(e).

> or approving an electronic data message or electronic document.[58]

A feature of the E-Commerce Act that is peculiar to electronic signatures is found in section nine. It provides for disputable[59] presumptions in that electronic signatures are presumed to be:

1. The electronic signature is the signature of the person to whom it correlates; and
2. The electronic signature was affixed by that person with the intention of signing or approving the electronic document unless the person relying on the electronically signed electronic document knows or has notice of defects in or unreliability of the signature or reliance on the electronic signature is not reasonable under the circumstances.

Just the same, the E-Commerce Act also provides for legal recognition of an electronic signature as the functional equivalent of the signature of a person in a written document provided that it is proved by showing that a prescribed procedure, not alterable by the parties interested in the electronic document, existed, subject to the enumerations in section eight of the said law.[60]

58. *Id.* § 11, first par (a).
59. TECHNOLAWGY, *supra* note 18, at 75 ("The section does not expressly provide that the presumptions are disputable but one author comments that the presumptions are disputable.").
60. ELECTRONIC COMMERCE ACT OF 2000, § 8 provides:

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

3. Acts Punished Under E-Commerce Act

In Section 33 of the mentioned law, there are three types of offenses that are punished. The first offense punished by the E-Commerce Act is unauthorized access to a computer system; the second is that of piracy; and the third refers to violations of the Consumer Act[61] "through transactions covered by or using electronic data messages or electronic documents."[62]

There are two general kinds of offenses committed against a computer system. The first kind is referred to as *hacking* or *cracking*, which is defined as an *unauthorized* access into or interference in a computer system or server or information and communication system.[63] The second kind pertains to "*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 documents."[64]

The first kind of hacking or cracking is straightforward. As long as access to a computer system is unauthorized, it falls under this category. However, there is no definition of what *unauthorized* is under the E-Commerce Act. This is a very delicate term when applied to computer systems because of the latter's extraordinary capabilities and must therefore be clarified.

To illustrate, access to one computer system may have been given to an employee, but if the computers in their workplace are all connected through their internal network, the same employee can access all the other computers that are linked to their network. There is a remedy to such situations. The system administrator(s) can modify the computer policy of their company and restrict the access from one computer to another through simple modifications in the main system or the server. In such a situation, can the employee who accesses a computer linked to his assigned terminal in the company claim that he was authorized to do so? The answer to this would depend on the computer use policy of the company. If access to other computer terminals is prohibited or limited by the company policy, then clearly, access to a different computer within the network is unauthorized. Hence, the vagueness of *unauthorized* can be remedied by a well-defined computer policy.

61. ELECTRONIC COMMERCE ACT OF 2000, § 33.

62. *Id.*

63. *Id.* at § 33 (a) (emphasis supplied).

64. *Id.* (Emphasis supplied).

However, if the call for interpretation of the term arises outside of a company setting, there is no possibility of looking to a computer policy for clarification. For example, person A accidentally accessed person B's personal computer. Both were linked to the internet during which person A was exploring the functions of some software specifically developed for entering other systems or *exploiting* another system. Should B file a complaint against A for the latter's intrusion into B's system, and claim that A violated section 33 of the E-Commerce Act? A can easily claim that his access to B's system is not authorized. This is because most operating systems, one of the more popular being Microsoft Windows, have known vulnerabilities and such vulnerabilities are not concealed from the public. Those who are more knowledgeable of the operating system concerned are able to take advantage of these vulnerabilities. Can the more knowledgeable not claim that he was authorized by the owner of the computer system which was accessed, because use of the product means implied consent to the vulnerabilities to which the system is subject?

A more complicated defense for A would be that there is implied consent on the part of B for other people to access his or her system by reason of the latter's connection to the Internet. This is because a connection to the Internet can only be maintained if some ports of the system are open, and these are the very same ports through which unknown users can access another person's computer.[65] The above account of the possible issues that would arise out of the lack of definition of unauthorized access is just a sampling of how malleable a computer system is. Hence, it behooves the legislature that the term be defined so as to limit a barrage of defenses from a party who has knowledge of a computer's intricacies and who desires to worm out of the offense imputed against him under the E-Commerce law.[66]

The second kind of hacking or cracking is more intricate than the first. It must have as its object the following: to corrupt, alter, steal, or destroy. In short, the person gaining access must have the intent as mentioned. The said person must make use of a computer, or any other similar information/communication device. In addition, the access must be made without the knowledge and consent of the owner of the computer or information/communication system. If the owner has either knowledge or consent, then the person who gained access to the computer or information/communication system cannot be held accountable for the second kind of hacking or cracking. Lastly, the access must result in the

65. *See generally* KEVIN MANDIA, CHRIS PROSISE AND MATT PEPE, INCIDENT RESPONSE AND COMPUTER FORENSICS (2003 2d ed.).

66. As of this writing, a cyber crime bill is pending with the Congress. Hopefully, it would provide a more precise definition of hacking or cracking in order that erring individuals may be prosecuted against.

corruption, destruction, alteration, theft or loss of electronic data messages or electronic documents. Therefore, (1) the intent to corrupt, alter, steal or destroy, along with (2) damage to the system through either corruption, destruction, alteration, theft or loss of electronic data messages or electronic documents are essential elements for the second kind of hacking or cracking under the E-Commerce Act. If either of the two is not present, there is no offense. If for example, accidentally, a virus infected the computer and it caused damage, there is still no offense because of the absence of the element of intent. This is rightfully so, because a computer is property and the owner must be responsible for his property. He must protect the system from intrusion or introduction of viruses just as he would protect invasion of his home or any of his personal effects.

Some legal experts on the E-Commerce Act categorize the first offense into four categories: (1) unauthorized access; (2) interference; (3) authorized access, with intent to corrupt, alter, steal, or destroy and (4) introduction of viruses and the like.[67]

The second offense under the E-Commerce Act is piracy, which is defined as

> 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 read on protected works, through the use of telecommunication networks.[68]

The definition of piracy in the E-Commerce Act requires infringement of intellectual property rights. For this purpose therefore, one must look at the Intellectual Property Code of the Philippines[69] to determine whether or not piracy was committed.

The third offense under the E-Commerce Act consists of violations of the Consumer Act[70] and other pertinent laws through transactions using electronic data messages or electronic documents. The E-Commerce Act does not impose an additional or a different penalty for such class of offenses

67. *See* Jesus M. Disini and Janette C. Toral, THE ELECTRONIC COMMERCE ACT AND ITS IMPLEMENTING RULES AND REGULATIONS (2000).

68. ELECTRONIC COMMERCE ACT OF 2000, § 33 (b).

69. An Act Prescribing the Intellectual Property Code and Establishing the Intellectual Property Office, Providing For Its Powers and Functions, and For Other Purposes, Republic Act No. 8293 (1997) [INTELLECTUAL PROPERTY CODE].

70. ELECTRONIC COMMERCE ACT OF 2000, § 33.

but simply recognizes that violation of the Consumer Act can be committed through the use of electronic data messages or electronic documents, and the penalties shall be the same as provided in the Consumer Act.

B. The Rules on Electronic Evidence

The Rules on Electronic Evidence were issued pursuant to the memorandum submitted by the Committee on the Revision of the Rules of Court to reflect the changes on the rules on evidence brought about by the E-Commerce Act.[71]

A more notable provision of the said Rules is section two of Rule 2, which provides that the interpretation of such rules shall take into consideration the international origin of the E-Commerce Act. This implies that in case of ambiguity, construction shall also take into consideration the international meaning and/or procedure which may be applicable to the blurry provision of the Rules.

A quick look at the E-Commerce Act's provisions and the Rules on Electronic Evidence will reveal that most of the terms and definitions are almost identical or similar. However, some of the disparities in word use spell all the difference when dealing with the presentation of evidence in court.

The Rules on Electronic Evidence also adopted the *functional equivalent approach* in treating paper based documents: every rule of evidence embodied in the said rules which refer to a writing, document, record, instrument, memorandum or any other form of writing is deemed to include an electronic document.[72] An electronic document is regarded as the original if it is a printout or output readable by sight or other means, shown to reflect the data accurately.[73]

In contrast with the authentication procedure under the E-Commerce Act[74] as previously described, the authentication procedure for electronic documents in the Rules on Electronic Evidence is simpler: authentication can be proved by *any* of the following means:[75]

1. By evidence that it had been digitally signed by the person purported to have signed the same;

71. TECHNOLAWGY, *supra* note 18, at 94.

72. RULES ON ELECTRONIC EVIDENCE, § 1, Rule 3.

73. *Id.* Rule 4.

74. ELECTRONIC COMMERCE ACT OF 2000, § 7.

75. RULES ON ELECTRONIC EVIDENCE, § 2 (a)-(c), Rule 5 (emphasis supplied).

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

3. By other evidence showing its integrity and reliability to the satisfaction of the judge.

While worded differently, the effect is the same in that both the authentication procedures in the E-Commerce Act and Rules on Electronic Evidence have the same concerns. Both laws (1) protect the *integrity* of the document and (2) seek to have the electronic document become capable of being *displayed* to the judge who will then decide on its admissibility.

There is also a separate authentication procedure for electronic signatures. Any of the following may be presented for authentication:[76]

1. Evidence that a method or process was utilized to establish a digital signature and verify the same;

2. Any other means provided by law; or

3. Any other means satisfactory to the judge as establishing the genuineness of the electronic signature.

Again, the Rules on Electronic Evidence's provision is simpler than that found in the E-Commerce Act.[77]

The Rules on Electronic Evidence contains disputable presumptions regarding electronic signatures *and* digital signatures. As opposed to the E-Commerce Act, the Rules on Electronic Evidence make a distinction between electronic and digital signatures. The former[78] is broader and includes digital signatures.[79]

76. *Id.* at Rule 6.

77. *Compare with* ELECTRONIC COMMERCE ACT OF 2000, § 11(a).

78. RULES ON ELECTRONIC EVIDENCE, § 1(j), Rule 2 provides: *"Electronic signature"* refers to any distinctive mark, characteristics 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 procedure employed or adopted by a person and executed or adopted by such person with the intention of authenticating, signing or approving an electronic data message or electronic document. For purposes of these Rules, an electronic signature includes digital signatures.

79. RULES ON ELECTRONIC EVIDENCE, § 1(e), Rule 2 provides: *"Digital Signature"* refers to an electronic signature consisting of a transformation of an electronic document or an electronic data message using an asymmetric or public cryptosystem such that a person having the initial untransformed electronic document and the signer's public key can accurately determine: (i) whether the transformation was created using the private key that corresponds to the signer's public key; and (ii) whether the initial electronic document had been altered after the transformation was made.

The Rules on Electronic Evidence results in a new exception to the hearsay rule under Rule 130 of the Revised Rules of Court. In Rule 8 of the former, the hearsay rule is made inapplicable to records (1) made by a person with knowledge thereof, (2) kept in the regular course of business activity and (3) such records were made as regular practice. These three elements may be shown by the custodian of the records or other qualified witnesses.

Another innovative introduction by the Rules on Electronic Evidence is the allowance of electronic testimony.[80] Parties can now present testimonial evidence through electronic means after a summary hearing.

Lastly, the Rules on Electronic Evidence also take into consideration *ephemeral electronic communication* which refers to telephone conversations, *text messages*, chatroom sessions, streaming audio, streaming video, and other electronic forms of communication the evidence of which is not recorded or retained.[81] These type of communications are to be proven by the testimony of a person who was party to the same *or* has personal knowledge thereof.[82] But more importantly, evidence of ephemeral electronic communications may still be admitted in the absence of persons party thereto or having personal knowledge thereof. The Rules allow other "competent"[83] evidence to be presented and admitted.[84]

C. Reconciling Rules

With the presence of the Rules of Evidence in the Revised Rules of Court, the rules on admissibility embodied in the E-Commerce Act, and the Rules on Electronic Evidence, a confusing list of rules faces the legal community. The author asserts that these three seemingly conflicting rules can be harmonized. However, the author is also of the belief that modifications are required so that the rules become clearer and more specific. Pending the

80. *See* RULES ON ELECTRONIC EVIDENCE, Rule 10.

81. RULES ON ELECTRONIC EVIDENCE, § 1(k), Rule 2 (emphasis supplied).

82. *Id.* at § 2, Rule 11.

83. Evidence is competent when it is not excluded by law in a particular case. (VII RICARDO J. FRANCISCO, THE REVISED RULES OF COURT IN THE PHILIPPINES (1997 ed.)).

84. RULES ON ELECTRONIC EVIDENCE, § 2, Rule 11.

possible amendment of these rules, the existing rules shall be analyzed to come up with a reconciliation of the abovementioned three laws.

The analysis starts with Section Two, Rule Three of the Rules on Electronic Evidence, which provides that an electronic document is admissible in evidence if it complies with the rules on admissibility prescribed by the Rules of Court and related laws, and is authenticated in the manner prescribed by the said Rules. Thus, admissibility relies on:

1. Rules of Court provisions on admissibility;
2. Related Laws' provisions on admissibility – the E-Commerce Act falls under this;
3. Authentication in the manner prescribed in the Rules on Electronic Evidence.

The Rules of Court provide the general rules for admissibility of *any kind* of evidence. Hence, it also applies to electronic type of evidence. But because the legislature recognizes that evidence of the electronic type is unique, and therefore must be handled differently from the usual kind of evidence, some laws were enacted to specifically cover electronic media. The E-Commerce Act did *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*.[85] Meanwhile, the Rules on Electronic Evidence also provide for its own version of the best evidence rule and authentication procedure. Which between the E-Commerce Act and the Rules on Electronic Evidence should be followed for authentication and for the best evidence rule as applied to electronic media?

Going back to the admissibility provision of the Rules on Electronic Evidence in Section Two, Rule Three, we are faced with the enumeration of the Rules to govern admissibility:

1. Rules of Court provisions on admissibility;
2. Related Laws' provisions on admissibility – the E-Commerce Act falls under this;
3. Authentication in the manner prescribed in the Rules on Electronic Evidence.

Hence, the Revised Rules of Court shall still govern, aside from authentication and best evidence. For authentication and best evidence, both the E-Commerce Act and Rules on Electronic Evidence govern. But what of their different wordings?

85. ELECTRONIC COMMERCE ACT OF 2000, §7, last par. (emphasis supplied).

One must take notice of the intent and fundamental concern of the two laws when it comes to authentication and best evidence. That is, both laws are concerned with the integrity of the document and its capability of being shown to the judge. Hence, the author suggests that a look at the Rules on Electronic Evidence must be made. This shall not run counter to the provisions of the E-Commerce Act, as both essentially state the same goals, only that the former is easier to understand and more convenient for both the litigant and the judiciary.

III. SURVEY OF PHILIPPINE CASES

In the 1991 case of *People v. Burgos,* [86] the prosecution sought to present a computer programmer to print out in court the material encoded in certain diskettes seized from private respondents by virtue of a private warrant. The Regional Trial Court (RTC) judge disallowed the same on the ground that these could be "manipulated."[89] In his comment, the judge said he did not allow the computer printout because it is subject to manipulation, and thus, would be prejudicial to the rights of the accused.[90] The Supreme Court, however, allowed the computer printout.[91] The Supreme Court observed that the mere fact that the diskettes were in the possession of the prosecution did not mean that it was tampered with, as suggested by the respondent judge. There were no testimonial or physical evidence of tampering presented to support this view. The Supreme Court then upheld the presumption of regularity in the performance of official duty.[92] It further advised that the apprehension regarding the possible manipulation of the diskettes and its contents can be "relieved by designating a competent person agreeable to both parties, and especially to respondent judge, who can perform the task of printing out the contents of the diskettes."[93]

As for the private respondents' contention that the diskettes should be inadmissible because these items were not included in the search warrant, the court found that the diskettes were *sufficiently described in the warrant.*[94] The

86. 200 SCRA 67 (1991).

87 Anti-Subversion Act, Republic Act No. 1700 as amended by Executive Order No. 276 dated July 15 1987.

88 200 SCRA 67.

89. *Id.* at 71.

90. *Id.*

91. *Id.* at 72.

92. *Id.*

93. *Id.*

94. *Id.* (emphasis supplied).

warrant authorized the search and seizure of "computer machine used in printing seditious or subversive literature."[95] The court opined that the cited phrase necessarily includes the diskettes into which data is encoded and stored, such as those seized in the present case on the same occasion that the computer itself was seized, because a computer system cannot store or print out any data without diskettes.[96] It went further and said that diskettes are deemed integral parts of a computer system, as input-output devices or peripherals.[97] This was in 1991.

Today, other storage media are used such as Iomega zip drives, thumb drives or flash disks, Compact Flash Cards, Memory Stick, MMC Card, SD Card, CD-RWs and other magnetic or optical storage. The options are numerous, and with all due respect to the Supreme Court that decided *Burgos,* these storage media *including the diskettes* they were referring to at that time, are *not* integral parts of a computer system. These facilitate storage, but they are not absolutely necessary for a computer system to function.[98] The files that can be contained on these storage media can be mere replicates of files created in a program residing and operating within the computer system. The source computer for the files stored in the storage medium can be more than two different computer systems, since most storage media are now compatible with most computer systems provided they have the proper ports in which the storage medium shall be inserted (such as floppy diskette drive, Compact Disk Drive, or Universal Serial Bus [USB] Drive). Besides, most computers are equipped with a built-in storage. Hence, the notion that a computer system cannot store or print data without a diskette or any other (external) storage media for that matter, must fail. Assuming that a competent person was presented to show the reliability and integrity of the diskettes, the same are still inadmissible because they were illegally obtained, in violation of sections two and three of Article III of the Constitution.[99]

Five years later, another case decided by the Supreme Court tackled, among other issues, electronic information. *IBM Philippines Inc. v. National Labor Relations Commission (NLRC)*[100] dealt with electronic mail, more popularly known as e-mail. The private respondent was about to be terminated on grounds of habitual tardiness and absenteeism. The private respondent claimed he was not given opportunity to be heard,[101] which, of

95. *Id.*

96. *Id.* at 73.

97. *Id.* at 73.

98. *See generally* TECHNOLAWGY, *supra* note 18.

99. *See* Lim, *supra* note 45.

100. 305 SCRA 592 (1999).

101. *Id.* at 595.

course, was denied by the petitioners who asserted that the private respondent was "constantly told of his poor attendance record and inefficiency through the company's internal electronic mail (e-mail) system."[102] Printouts of the alleged messages were attached to the petitioners' position papers. While the labor arbiter dismissed the complaint, the NLRC reversed and ordered reinstatement, and ruled that "the computer printouts which petitioners presented in evidence to prove the private respondent's attendance was poor were insufficient to show that the latter was guilty of habitual absences and tardiness."[103] IBM Philippines appealed to the Supreme Court, and attributed two errors on the part of respondent NLRC: (1) in holding that no just cause existed nor was there observation of due process because the printouts which prove just cause and due process are not admissible in evidence,[104] and (2) in holding that even assuming that the computer printouts were admissible, they failed to satisfy due process.[105] The Supreme Court ruled that the computer printouts "afford no assurance of their authenticity because they are unsigned."[106]

From an analysis of these two landmark cases decided prior to the issuance of the Rules on Evidence, two basic concerns come to fore, namely *reliability* and *authenticity*.

The crux of the matter that can be gleaned from these early cases is whether these two identified issues are now sufficiently addressed by our laws.

In 1991, the *Burgos* court allowed the printing in court of the contents of seized diskettes, alleviating doubts as to the possible tampering of the diskettes by stating that the parties can easily designate a competent person who can perform the task of printing the contents of the diskettes. The same court also ruled that the diskettes were admissible in evidence, saying that these were sufficiently described in the warrant.[107] In 1999, the Supreme Court disallowed printouts of e-mail as evidence as these do not afford an assurance of their authenticity. These two cases served as doctrines on presentation of electronic evidence prior to the enactment of the E-Commerce Act and the Rules on Electronic Evidence. At that time, what was of utmost importance was that the offering party can show to the court that the electronic evidence they

102. *Id.* at 596.

103. *Id.* at 599.

104. *Id.*

105. *Id.* at 600.

106. *Id.* at 601.

107. *Burgos*, 200 SCRA at 72.

seek to present is authentic and not manipulated with, and this can be done by presenting testimonial evidence of person(s) having personal knowledge of the document sought to be presented. However, *Burgos* must be read carefully as it is dangerous to assume that a warrant for a computer includes the diskettes and its accessories. This is almost tantamount to a blanket warrant. Though instructive, the simplistic requirement laid down in *IBM Philippines* is secondary to the parameters for authentication laid down in the Rules on Electronic Evidence.

There were also other cases where electronic evidence was presented. *People v. Ordoño*[108] is a rape-slay case where accused Pacito Ordoño and Apolonio Medina were interviewed by a radio station reporter, Roland Almoite. Both individually narrated their participation in the commission of the alleged crime. The other extrajudicial confessions of the accused were rendered inadmissible in evidence so the court turned to the interview taken by Almoite. The prosecution offered the taped interview to form part of the testimony of Almoite and to prove through *electronic device* the voluntary admissions that they indeed raped and killed the victim.[109] The defense objected to the presentation of the tape on the ground that it could have been easily spliced and tampered with.[110] No mention was made of authentication of the tape.

People v. Williams[111] is a case for violation of the Dangerous Drugs Act.[112] As alibi, accused Nzenza claimed that he could not have committed the offense as he did not have any checked-in luggage as claimed by the prosecution. To verify this, an employee of Philippine Airlines furnished a printout of a passenger manifest – a computer record of passengers and corresponding details. It indicated that Nzenza was passenger number 37 of Swiss Air Flight No. SR-177, and three pieces of luggage with corresponding baggage identification numbers were also recorded under his name. The court did not give credence to this evidence: "the passenger manifest, standing alone and without the testimony of the employee who recorded the seat number and number of checked-in baggage, is hearsay."[113] Here, it is again evident that authentication through the testimony of a person having personal knowledge of the computer record (passenger manifest) is necessary.

108. 334 SCRA 673 (2000).

109. *Ordoño,* 334 SCRA at 691.

110. *Id.*

111. 357 SCRA 124 (2001).

112. Dangerous Drugs Act of 1972, Republic Act No. 6425 (1972).

113. *Williams,* 357 SCRA at 138.

What can be considered a landmark case in the application of the Rules on Electronic Evidence is *Nuez v. Cruz-Apao,*[114] an administrative case for dishonesty and grave misconduct. Respondent is an Executive Assistant II of the Acting Division Clerk of Court of the 15TH Division of the Court of Appeals (CA). Complainant Zaldy Nuez has a case lodged in the Court of Appeals, which has been pending for two years. In his desire to have a speedy disposition of the said case against Philippine Amusement and Gaming Corporation (PAGCOR), he informed the respondent of his case thinking that he would be given advice for early resolution. Respondent allegedly told complainant that a favorable and speedy decision of his case was possible but the person who was to draft the decision was asking for the amount of one million pesos in return. Complainant sought the help of the television show, *Imbestigador,* in order that the proper case may be filed against the respondent. Through their help, he was able to gather ample evidence, among which were text messages from the respondent, alluding to the same one-million-peso bribe in exchange for a favorable decision in the complainant's favor. The text messages were admitted in court, pursuant to the provisions of the Rules on Electronic Evidence regarding the admissibility of ephemeral electronic communications, which include text messages. Section 2 Rule 11 requires the presentation of "the testimony of a person who was a party to the same or who has personal knowledge thereof."[115] The complainant himself testified to his personal knowledge of the text messages and respondent admitted that the cellular phone number reflected in complainant's [cellular phone] from which the messages originated was hers.[116] *The Rule is clear, and it was simply applied by the court.*

IV. CELLULAR PHONES

The increasing use of cellular phones as a means of communication has made them an important piece of evidence in many legal cases. Indeed, cellular phones lend convenience and ease in daily transactions. It will not be surprising that in the coming days, cellular phones will be widely used for e-commerce and the relevance of cellular phone evidence will assume greater importance.

Since a cellular phone is an electronic device there are several aspects of the E-Commerce Act and the Rules on Electronic Evidence that are applicable and relevant in terms of evidence collected therefrom.

114. A.M. No. CA-05-18-P, April 12, 2005.

115. RULES ON ELECTRONIC EVIDENCE, Rule 11, §.

116. *Nuez,* 455 SCRA 288.

These are early days of using cellular phone evidence and there is a high possibility that an imperfect understanding of the technology by the police, the lawyers and the judges may lead to imperfect judicial decisions.

It must be emphasized that electronic devices can be used as a source of evidence in *any crime*, and a cellular phone is an electronic device. A great amount of information can be derived from cellular phones and these can be relevant and pivotal evidence in various actions and/or proceedings, such as the numbers to which calls have been made from a given mobile with date and time, the contact information of all the individuals whose numbers are stored on the cellular phone, details of text messages sent and received, and even pictures taken using the camera-phone or sent to the phone.

Perhaps cellular phones and the electronic evidence that *could* be contained therein invited closer attention and analysis by reason of *Nuez*.

V. ISSUES SURROUNDING ELECTRONIC EVIDENCE

One of the most significant requirements for admissibility of any evidence is integrity. The same is true for electronic evidence, more so because of its susceptibility to tampering and manipulation. Integrity of evidence is shown through authentication in the process prescribed by law.

In providing for the rules on authentication, Section 11 of the E-Commerce Act gives great room for *other* means of authentication. It uses the phrase "among *other* ways."[118] It has been suggested that "other ways" refer to testimonial sponsorship, circumstantial evidence, authentication via an intermediary and any other method mutually agreed upon by the parties.[119] However, "other ways" is a very broad term that can be interpreted to mean a magnitude of ways. Needless to say, this has to be clarified or expounded upon.

Another ambiguous area is found in the requirement for authentication of electronic data messages and electronic documents which call for proof of *appropriate security procedure*. It is a technical term that should have been defined, but the vagueness of the term is not fatal to the authentication procedure. As mentioned, parties can authenticate evidence in other ways. What these ways are is left to the imagination and creativity of counsels who are free to consult or enlist the aid of computer forensics experts.

117 A.M. No. CA-05-18-P.

118. ELECTRONIC COMMERCE ACT OF 2000, § 11, ¶ 1 (emphasis supplied).

119. Lim, *supra* note 45, at 366-367.

On the other hand, there is also a misconception that must be corrected in the Rules on Electronic Evidence. Most practitioners believe that electronic documents cannot be presented if neither the sender nor the recipient may testify. However, it is clear in section 2, Rule 5, that the individual coming to authenticate the proffered evidence need not be a party to the electronic document. The provision does not make reference as to who may authenticate. He simply must have *personal knowledge* of the electronic file. The systems administrator of the company, if any, can be such person. Supposing that in the *IBM Philippines*[120] case, an expert of the company who handled the electronic mail communications was presented, then the requirement of the court in *Burgos*[121] of a "competent person" could have been satisfied.

Commentators also report that during the discussion of the authentication provisions of the E-Commerce Act, Senator Loren Legarda-Leviste posed a question as to who will perform the process of authentication. Senator Magsaysay replied that "the parties themselves may do so or in the alternative, engage the services of third party authenticators."[122] Taking into consideration that the Rules on Electronic Evidence were intended to *reflect* the changes in the Rules on Evidence which were brought about by the E-Commerce Act, the opinion of Sen. Magsaysay on the authentication procedure of the E-Commerce Act may also be applied in the interpretation of the authentication procedure outlined in the Rules on Electronic Evidence.

The issue of *chain of custody* is also an issue of integrity. The parties who wish to present electronic evidence must ensure that the data they present in court are unaltered. The process within which they handle the electronic evidence must be thorough and precise, yet careful and meticulous. Part of this process is documenting all the steps performed on the electronic evidence to be presented in court. This documentation must include all the individuals who handled the evidence to establish the chain of custody.

Meanwhile, the best evidence rule is primarily embodied in the Revised Rules of Court, which provides that when the subject of the inquiry is the *content of a document*, no evidence shall be admissible other than the *original* itself, subject to certain exceptions.[124] Both the E-Commerce Act[125] and the

120. IBM Philippines v. NLRC, 305 SCRA 592 (1999).

121. *Burgos*, 200 SCRA 67.

122. Disini and Toral, *supra* note 67, at 20.

123 Revised Rules of Court, § 3, Rule 128.

124. § 3, Rule 128. Original document must be produced; exceptions. – When the subject of the inquiry is the contents of a document, no evidence shall be admissible other than the original document itself, except in the following cases:

Rules on Electronic Evidence[126] provide for rules to govern the best evidence with regard to electronic information. The dilemma lies in which rules to follow in case of proceedings and actions (of any type) in which electronic media is sought to be presented.

The author puts forth the following suggestion: As a general rule, the Revised Rules of Court shall govern for matters other than authentication and best evidence. However, for authentication and best evidence, both the E-Commerce Act and Rules on Electronic Evidence shall apply. One must take note of the intent and fundamental concern of the two laws when it comes to authentication and best evidence: both are concerned with the integrity of the document and its capability of being presented to the judge. Hence, the author suggests that a look at the Rules on Electronic Evidence must be made. This shall not run counter to the provisions of the E-Commerce Act, as both essentially state the same goals. However, the former is easier to understand and more convenient for both the litigant and the judiciary.

Hence, the provision on best evidence in the Rules on Electronic Evidence states that an electronic document shall be considered the original if it is a printout, or an output readable by sight or other means, shown to reflect the data accurately.[127]

VI. AMERICAN JURISPRUDENCE

Some cases decided in the United States shall be surveyed and the doctrines pertinent to electronic evidence shall be culled from the said cases due to the dearth of Philippine jurisprudence on the matter. As electronic evidence is fairly unexplored territory in the Philippines, it is also a new form of evidence in the United States. However, in the latter, there are numerous

a. When the original has been lost or destroyed, or cannot be produced in court, without bad faith on the part of the offeror;
b. When the original is in the custody or under the control of the party against whom the evidence is offered, and the latter fails to produce it after reasonable notice;
c. When the original consists of numerous accounts or other documents which cannot be examined in court without great loss of time and the fact sought to be established from them is only the result of the whole; and
d. When the original is a public record in the custody of a public officer or is recorded in a public office.

125. ELECTRONIC COMMERCE ACT OF 2000.

126. RULES ON ELECTRONIC EVIDENCE, § 1, Rule 4.

127. *Id.*

cases wherein electronic evidence was successfully presented, and thus present useful and instructive doctrines on the presentation of electronic evidence. Because of this, and of the fact that the E-Commerce Act was based on international model(s), the above-described doctrines shall be presented.

In *U.S. v. Tank*[128] the defendant was being prosecuted for sexual exploitation of a child for the purpose of producing a sexually explicit video for distribution. Tank was a member of the *Orchid Club*, an internet chat room involved in the discussion, trading and production of child pornography. Ronald Riva, another member of the Orchid Club, was arrested for child molestation. A search of Riva's home and computer files revealed thousands of pornographic pictures of children and computer text files containing recorded online chat room discussions that took place among members of the Orchid Club. These evidence implicated Tank and other members of the Orchid Club. Tank moved to suppress the chat room logs[129] and argued that the government failed to present sufficient foundation:

> Tank objected that there was no foundation for admission of the chat room log printouts into evidence because: (1) they were not complete, and (2) undetectable material alterations, such as changes in either the substance or the names appearing in the chat room logs, could have been made by Riva. The district court ruled that Tank's objection went to the evidentiary weight of the logs rather than to their admissibility, and allowed the logs into evidence.[130]

The federal court, in reviewing the district court's decision explained that the government has to make a mere *prima facie* showing of authenticity of offered evidence, and that such requirement was fully satisfied. In the hearing, Riva explained how he created the logs with his computer and even said that the printouts of the logs "appeared to be an accurate representation of the Orchid Club conversations."[131] The federal court also found that a link between Tank and the chat room logs were made, as Tank himself admitted to the use of the screen name Cessna when he participated in the chat room conversations.

Authentication of evidence through the testimony of a competent and qualified witness is key to its admissibility. The question of *who* can present testimony to such effect looms. *U.S. v. Mooring*[132] illustrates how the person

128. 200 F.3d 627 (2000)

129. Record of conversations that took place in the chat room.

130. 200 F.3d at 631.

131. *Id.*

132. 137 F.3d 595 (1998).

who knows the evidence best testified for the purpose of its authentication. The Moorings were suspected of growing marijuana through the use of increased heat in some portions of their home. The FBI agent who personally retrieved and printed the records of the defendants' electric bill as evidence of growing marijuana also personally testified in court with respect to the printouts of the electric bill.

The case of *Armstrong v. Executive Office of the President*[133] demonstrates what best evidence is *not*. In that case, certain paper printouts of federal records consisting of documents created by executive agencies' electronic communication systems were presented in court. The court ruled that indeed, the records in the computer are considered *records* as defined by the Federal Records Act (FRA). However, the printed copies are not *copies*, since the executive offices concerned openly admitted that these printouts were just extra copies kept for the purpose of reference. The court even observed that based on the court record (evidence), the computer record and the printouts cannot be considered identical twins but merely "kissing cousins."[134] The Philippines does not have a FRA, but the Rules of Court[135] allows *copies* of the original document to be presented as originals, and the Rules on Electronic Evidence[136] as well allows copies as originals, subject to some requirements.

A typical example where an expert was allowed to testify on computer forensics activities is *U.S. v. Hilton*,[137] where the defendant was indicted for possession of computer disks, tapes, and other material that contained three or more images of child pornography that had been transported in interstate

133. 1 F.3d 1274 (1993).

134. *Id.* at 1283.

135. REVISED RULES OF COURT, § 4 (a) Rule 130: "Original of document – (b) When a document is in two or more copies executed at or about the same time, with identical contents, all such copies are equally regarded as originals."

136 RULES ON ELECTRONIC EVIDENCE, § 2, Rule 4: "*Copies as equivalent of the originals.* – When a document is in two or more copies executed at or about the same time with identical contents, or is a counterpart produced by the same impression as the original, or from the same matrix, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduces the original, such copies or duplicates shall be regarded as the equivalent of the original. Notwithstanding the foregoing, copies or duplicates shall not be admissible to the same extent as the original if:

(a) a genuine question is raised as to the authenticity of the original; or

(b) in the circumstances it would be unjust or inequitable to admit a copy in lieu of the original.

137. 2000 WL 894679 (D.Me.) (not reported in F.Supp.2d).

and foreign commerce by computer via the internet.[138] The parties stipulated in the beginning of the trial that Special Agent Marx, who handled hard disks and files owned and used by the defendant, is a computer forensics expert. Thus, later on in the trial, he was allowed to testify and interpret the data he yielded from his examination.

The court in *U.S. v. Scott-Emuakpor*[139] was less stringent but nevertheless vigilant. The search was conducted by Secret Service Agent Baisel with four companions who were authorized under the warrant to seize computer files that disclosed the names and addresses of persons who participated in the fraudulent investment scheme for which the defendants were being held accountable. Baisel seized a laptop computer which was later examined off-site by Agents Christy and Walsh. The defendants sought to prevent the two latter agents from testifying, on the basis that they were not present during the search and because they were not computer experts. The court rejected these arguments and held,

> The question before the Court at this time is not whether these witnesses have the expertise, for example, to develop sophisticated software programs. The question is whether they have the skill to find out what is on a hard drive or a zip drive. Apparently, they have this skill because they determined what was on the drives.[140]

Further, the two agents are to be considered expert witnesses under their Federal Rules of Evidence.[141] Said the court, "[b]y analogy, a person need not be an expert on English literature in order to know how to read."[142]

The author does not discount the informative value of the mentioned two cases, but she is of the opinion that *People v. Lugashi*[143] is a key case that challenged experts' testimonies. Defendant rug merchant was indicted for grand theft and four counts of receiving payment for items falsely represented to credit card issuers as having been furnished.[144] The person testifying to evidence obtained through computer forensics was admittedly not an expert, but the court took him as an expert witness for purposes of the said case: "[he] who generally understands the system's operation and possesses sufficient knowledge and skill to properly use the system and

138. *Id.* at 1.

139. 2000 WL 288443 (W.D.Mich.) (not reported in F.Supp.2d).

140. *Id.* at 13.

141. Fed. R. Evid. 702.

142. *Supra* note 140.

143. 205 Cal.App.3d 632 (1988).

144. *Id.*

explain the resultant data, even if unable to perform every task from initial design and programming to final printout, is a 'qualified witness.'"[145]

Care must be made in the choice of expert. Since Computer Forensics is unexplored territory in the Philippines, there is not much of a choice, but the importance of a reputable computer forensics team must be stressed. In *Gates Rubber Co. v. Bando Chemical Industries*[146] the plaintiff, on grounds of chronic and continuous destruction of evidence, sought discovery sanctions against the company, which allegedly stole trade secrets.

In order to collect electronic information from computers in Bowling Green, a manufacturing plant of Bando, the court appointed a certain Mr. Scheideman as "court-appointed technician." In question were the contents of Kessinger's computer in Bowling Green. Plaintiff alleges that the contents of Kessinger's computer, known as the 2007, were replaced or overwritten by contents of another computer known as the 1100. Gates' counsel claims that this was done with the intent of destroying evidence. However, evidence submitted by Scheideman does not state that the computer numbered 2007 was owned or used by Kessinger. This fact prompted the court to delve deeper into this matter.

Gates' forensic expert Robert Wedig testified that transfer of files from computer number 1100 to 2007 indeed occurred. He even illustrated that computer 1100 was commonly used by Pat Smith, a secretary in Bowling Greens. He demonstrated that the transfer of files from 1100 to 2007 happened before they received word that a site inspection of Bando's Bowling Greens plant would be made. Further, he was able to show to the court that computer number 2007 is available for use not only by Kessinger but by other employees as well, including Pat Smith. Wedig offered information explaining the failure of Scheideman in resurrecting the deleted files in the Bowling Greens computers, including 2007. Wedig explained that Scheideman committed an error in the operation of "Norton Unerase," and that proper operation would have revealed that the computers, in fact, contained deleted files. He offered a number of facts in support of this.[147] Voorhees, the expert of Gates, did not offer a timely explanation to Wedig's claims.

The court believed Wedig, found him to be extremely learned, and was not persuaded by argument from counsel (Gates') to reject Wedig's findings and opinions.[148] As for Scheideman, the court clarified that it is not required

145. *Id.*

146. 167 F.R.D. 90.

147. *Id.* at 120.

148. *Id.*

to ratify or adopt his findings or conclusions simply because he was court-appointed.[149] The court also found that most of the search conducted by Gates' party were conducted by counsel, instead of computer forensics experts, as opposed to the search conducted by Bando's party which was performed by Wedig. As a result, the court admonished Gates:

> the circumstances required that Gates utilize the technology which would produce the most complete and accurate picture of the evidence, and Gates failed to ensure that this was done. Where any uncertainty exists with regard to the results of this failure by Gates, Gates should suffer the consequences of that failure.[150]

This does not indicate that every computer search must be conducted by computer forensics experts and not by lawyers. What is important is that the most *effective* and *accurate* technology be used. It can be performed by counsel, as long as he or she is prepared to tender evidence of his or her knowledge to the court. This signifies that the chosen computer forensics team/expert must also be abreast with the most effective and accurate technology, or if the counsel decides to perform the forensic task himself (perhaps as a cost-cutting measure, or for whatever reason), he should consult an expert first.

VII. RECOMMENDATIONS

The recommendations in this Note shall be divided into the three stages of Computer Forensics, the process through which electronic evidence is collected and preserved for the purpose of presentation in court, and the gaps in the judicial system which should be addressed to make way for electronic evidence.

A. Preliminaries – Collection and Investigation of Electronic Evidence

The foremost rule is that electronic material can be subject of forensics if it is relevant to a fact in issue and a plausible basis for its collection can be given.[151] Computer forensics must also be carried out in the least intrusive manner possible.[152]

The rules for search and/or seizure must be distinguished according to the party performing the task. If it is to be performed by the government, the rules embodied in the Fourth Amendment of the U.S. Constitution, or

149. *Id.* at 121.

150. *Id.*

151. Fennell v. First Step Design, Ltd., 83 F.3d 526 (1st Cir. 1996).

152. Strasser v. Yalamanchi, 669 So.2d 1142 (Fla.App. 1996).

Section two, Article three of the Philippine Constitution must be followed. Probable cause for the issuance of a warrant must be well-grounded, and not merely alleged, even if clothed in a notarized affidavit.[153] Once issued, a warrant must be read carefully. It does not amount to authority to search all computers, their hard drives and accessories. The terms of the warrant shall dictate the limits of the search.[154] A separate warrant must be requested and issued therefor.

Prior to a computer forensics operation for the gathering of electronic evidence, the party to conduct the search is expected to address feasibility issues by submitting to the court and other parties their feasibility assessment.[155] The court may appoint a computer specialist to serve as officer of the court, and in case such officer accessed material covered by attorney-client privilege, it may not be admitted as evidence.[156] All processes performed shall be documented and completed within the time frame provided for by the court.[157] The same process may be adopted in warrantless searches.

Warrantless searches of computers and/or electronic devices by the government are also covered by the Fourth Amendment as evinced by the abundance of U.S. jurisprudence on the matter. [158] By inference, the protection in the Philippine Constitution also extends to warrantless searches of computers and/or electronic devices such that it must submit to the reasonable expectation of the privacy test.

The search or production of evidence, if ordered by the court, must also minimize disruption in the business of the party being searched.[160] Proof of

153. *See* United States v. Brunette, 256 F.3d 14 (1st Cir. 2001); United States v. Hernandez, 183 F.Supp. 2d 468 (2ND Cir. 2002) and United States v. Simpson, 152 F.3d 1241 (10th Cir. 1998).

154. *See* United States v. Carey, 172 F.3d 1268, 1272 (10th Cir. 1999); State v.Schroeder, 613 N.W.2d 911 (Wis. App. 2000) and United States v. Gray, 78 F. Supp. 2d 524 (E.D. Va. 1999).

155. Playboy v. Welles, 60 F.Supp.2d 1050, 1054 (1999).

156. *Id.*

157. *Id.* at 1055.

158. Kyllo v. United States, 533 U.S. 27 (2001).

159 *Kyllo,* 533 U.S. 27.

160. Simon Property Group v. mySimon Inc., 194 F.R.D. 639 (2000).

relevance of the electronic discovery must be presented to court to elicit a *subpoena* or a production of evidence order from the court.[161]

B. Electronic Evidence Prior to Presentation in Court

Retention policies of some parties may be reviewed. The policies are usually allowed by courts as long as it is reasonable, *bona fide* and not issued in bad faith or issued to avoid its being presented in court during litigation.[162] Knowledge of relevance of the electronic documents in litigation causes the *duty* to preserve the document to set in.[163] In case some relevant or material electronic evidence are spoiled or destroyed, sanctions may be imposed under Federal Rules in the U.S., and prejudice caused to the requesting party, intent of the person responsible for spoliation and degree of relevance of the destroyed material to the case are the most important considerations in determining the sanction to be imposed.[164] It is suggested that a system of sanctions be integrated in the Rules of Court to convey to parties how integral evidence can be and how detrimental it would be to a case if destruction is taken lightly. Further, avoiding the destruction of potential evidence is all the more significant when evidence is in electronic form. Given the malleability and susceptibility to tampering of electronic data, efforts should be made to ensure the integrity and authenticity of these data.

C. Presentation of Electronic Evidence in Court

Finally, it should be remembered that courts do not commonly issue *subpoenas* or orders for production of electronic evidence without substantial showing of its relevance in the case. Statutory limits should be made to exist not only as against examination to be made by the government but also by private individuals, even if blessed with the court's order or the consent of the owner or person in control or in custody. This is an area for the consideration of the Philippine legislature. Without limits, privacy of individuals may be trampled upon. In this phase, the proper authentication of the electronic data is also significant. The Rules on Electronic Evidence provide for the process for authentication, which should be followed. This

161. *See Stallings,* 2002 WL 385566 (N.D.Ill.); 52 Fed.R.Serv.3d 1406 (Not Reported in F.Supp.2d) and *In Re: General Instrument,* 1999 WL 1072507 (N.D.Ill.) (Not Reported in F.Supp.2d).

162. *See* Lewy v. Remington Arms Co., 836 F.2d 1104 (1988); Carlucci v. Piper Aircraft Corporation, 102 F.R.D. 472 (1984); Mathias v. Jacobs, 197 F.R.D. 29 (2000).

163. Telecom International America v. At&T Corp., 189 F.R.D. 76 (1999).

164. Gates Rubber Co. v. Bando Chemical Industries, 167 F.R.D. 90 (1996).

would afford the court an opportunity to assess the integrity of the documents. For the part of the forensics team, the process they adopted in collecting and analyzing the electronic evidence must be in light of the rules on admissibility of electronic evidence so that they can easily demonstrate to the court the integrity and reliability of the evidence they gathered and now seek to present. The witness(es) to be presented for authentication must be competent and qualified under the Rules of Court. In the case of authentication of electronic communications, it would be desirable to present either of the parties thereto. But counsel should not lose heart if neither of the parties is available to testify, because the rules allow any person having *personal knowledge* of the electronic document to testify to its integrity. In the computer world, a person need not be a party to a communication to be considered as having personal knowledge of the electronic evidence. For instance, a systems administrator of a company can testify to an electronic mail sent through the company's internal network as he has personal knowledge that the system was actually used in sending the mail, especially if the network policy of the company allows or mandates the administrator to monitor each communication sent internally, as is usually the case in other countries. This also points to the fact that computerized business records may be presented as exception to the hearsay rule, for as long as these records can be authenticated through the testimony of a person who qualifies under the exception in Rule 8 of the Rules on Electronic Evidence.

The court and its judges must also be knowledgeable in Computer Forensics. They need not be experts, but they must be able to understand the rudiments of a computer and its operation. This will enable them to hear cases wherein electronic evidence is presented more effectively and efficiently.

D. Filling the Gaps in the Legal System

The laws must also be changed to answer the issues previously outlined. For authentication of electronic evidence, the process must be clear and must ensure that integrity shall be demonstrated to the court. The Rules on Electronic Evidence procedures are simple, but these must still be expounded upon. Misconceptions that only parties to an electronic communication can have personal knowledge of the electronic document involved must be downplayed through a more express and encompassing phrasing of the authentication procedure.

For the best evidence rule, the Rules on Electronic Evidence are already refined. However, doubts as to the possibility of presenting electronic originals must be allayed through nationwide education as to the capabilities of a computer. Authentication also involves the business records as an exception to the hearsay rule. As the public relies on business records on paper, they should also learn to rely on electronic records. This can be done

by adding "computerized business records," its definition and requisites to the list of exceptions to the hearsay rule in the Rules of Court. This will give no room for doubt. It was embodied in the Rules on Electronic Evidence but it is not given enough attention. Experts or individuals educated in the field of computer forensics must also be given the opportunity to testify in court to aid the integration of computer forensics in the legal system.

For discoverability, a limit to the *subpoena* in any kind of case and on the order for production of material evidence in criminal cases must be codified. Electronic data can contain greater private information than its paper counterpart and therefore must be protected from overbroad court order(s). This does not mean that the courts' judgments are not to be trusted, but this would enhance public trust in the judiciary because there are greater safeguards to the right to privacy.

It is also recommended that a study of the feasibility of putting up a National Computer Forensics Laboratory in the Philippines be made.

> There is no dedicated facility for computer forensics now existing in the Philippines. Admittedly there are a few computer data recovery laboratories being maintained by hardware vendors and information system service providers, but none is dedicated to the thorough, efficient and secure means of investigating computer crimes from initial discovery to expert witness testimony in a court of law. Hence the need for a National Computer Forensics Laboratory.[165]

Both the NBI and the PNP are equipped to perform computer forensics operations. However, it would be better to have a specialized facility. In line with the proposal for the creation of a Department of Information and Communications Technology, a computer forensics division can be created as part and parcel of the DICT. Computer forensics is an integral part of technology and the judicial system will benefit much from its integration in the Philippines. It is a fairly new mode of gathering evidence, but other countries have already adopted it.

The USA Patriot Act[166] specifically supports computer forensics. Section 816 thereof authorizes the expenditure of $50 million for the creation and support of regional computer forensic laboratories. The Philippines' DBM meanwhile has appropriated Php 3 billion for the proposed DICT.[167] With a very large national government debt, it may be said that the Philippines

165. TECHNOLAWGY, *supra* note18, at 119.

166. Uniting and Strenghtening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) [USA PATRIOT ACT].

167. *Supra* note 10.

better expend its money and national resources in other more worthwhile projects. But once the laboratory is established, it is expected to benefit the police officers, other law enforcement agencies, Information Technology professionals, legal professionals, the judiciary and other government agencies.[168] The benefits that will follow are worth every peso that will be spent for its establishment. The court and its judges must also be knowledgeable in computer forensics. They need not be experts, but they must be able to understand the rudiments of a computer and its operation. This will enable them to hear cases wherein electronic evidence is presented more effectively and efficiently. In line with this, it is recommended that an administrative agency be created for the purpose of supervising the creation and maintenance of a National Computer Forensics Laboratory. This agency shall be composed of individuals, preferably lawyers, who will be trained in computer forensics procedures. The agency shall be tasked to take care of the integration of computer forensics in the judicial system. Hence, they will be assigned to conduct seminars and trainings of judges, court personnel, public and private lawyers.

These proposals will require a large amount of time and resources. It is estimated that computer forensics will be entrenched as a part of the legal process in a gradual manner. The sporadic attempts at presentation of electronic evidence in court evince that the integration of computer forensics as a valuable tool for obtaining evidence will not be in the near future. Perhaps in fifteen or twenty years, tides will have changed in favor of computer forensics and the benefits it has to offer. Indeed, it has its limitations and disadvantages, and these must be safeguarded against especially when these can be utilized by unscrupulous individuals in obstructing the law and dispensation of justice.

The law must always change to adapt to societal changes. It would be inevitable that more and more people and organizations will use electronic devices, and, as a result, relevant evidence will come in electronic form. Thus, room must be made in the legal system for this upcoming and unique form of evidence.

It is necessary to amend and add to the rules on admissibility and to the right of privacy *now*. The gaps and ambiguities in the laws and rules relating to electronic evidence discourage its utilization in court, and the growth of crimes, offenses and violations of rights where electronic evidence may prove to be relevant cannot be brought to a halt.

168. TECHNOLAWGY, *supra* note 18, at 120.

Taruc v. dela Cruz: Conservatism in Reviewing Decisions of Ecclesiastical Tribunals

*Theoben Jerdan C. Orosa**

I. INTRODUCTION

The jurisdiction of the civil courts to review the decisions of ecclesiastical tribunals in suspending or expelling members from a church, religious society, or corporation is limited by primordial considerations of religious liberty and the principle of separation of church and state. Some of the considerations are well-settled, such as the right of the individual to associate

* '06 J.D., cand., Ateneo de Manila University School of Law; Member, Board of Editors, *Ateneo Law Journal*. His previous works include *Constitutional Kritarchy Under the Grave Abuse Clause*, 49 ATENEO L.J. 565 (2004) and *The Failed Computerization of the National Elections and the Nullification of the Automated Election Contract*, 49 ATENEO L.J. 258 (2004). He also co-authored *In Re Purisima: Competence and Character Requirement for Membership in the Bar*, 48 ATENEO L.J. 840 (2003) with Ms. Aimee Dabu *et al.*

Cite as 50 ATENEO L.J. 211(2005).