# Are We Ready for Another Love Bug? Delving into Cybercrime and Re-Examining the e-Commerce Act of 2000 and Other Pertinent Laws

*Bernard Joseph B. Malibiran*[★]



---

★ '08 J.D., Ateneo de Manila University School of Law, '02 B.S., University of Asia and the Pacific. He was a member of the Board of Editors (2005-2008) and the Executive Committee (2006-2008) of the *Ateneo Law Journal*. He was also the Lead Editor for Vol. 51, Issue No. 1 and for the *Ateneo Law Journal* Citation Primer. His previous works in the *Journal* include *Psychological Incapacity Revisited: A Review of Recent Jurisprudence*, 52 ATENEO L.J. 392 (2007) and *Examining Executive Privilege in Light of Executive Order No. 464: A Comment on Senate of the Philippines, et al. v. Ermita, et al.*, 51 ATENEO L.J. 212 (2006). This Note is an abridged version of the author's Juris Doctod thesis on file with the Professional Schools Library, Ateneo de Manila University. The author would like to acknowledge the invaluable help provided by Atty. Christopher L. Lim, Atty. Lorenzo U. Padilla, and Ms. Carla R. Silverio.

*Cite as* 53 ATENEO L.J. 32 (2008).

## I. INTRODUCTION

### *A. Background of the Study*

4 May 2000 awakened the world to a reality that has so often been neglected or ignored in this present highly computerized age. It was a Thursday and, for many people, it was just another day of work. Stockbrokers, graphic artists, lawyers, engineers, and journalists alike across the globe all reported for work that day with new e-mails to read and reply to. Little did they know that a worldwide surprise was about to meet them, for in their inbox, among the usual e-mails from friends and colleagues, was one that contained the words "ILOVEYOU" in the subject heading. As no possible harm could come from an innocent-looking e-mail with "ILOVEYOU" in the subject line, especially if it is coming from a friend or colleague, people — some of them perhaps lonely in their little workspaces or cubicles in the office, and others, just plain curious — could not resist opening the e-mail. In the e-mail was an attachment labeled "LOVE-LETTER-FOR-YOU.TXT.VBS." From the attachment, the ".TXT" must mean that the attachment was a text file, and indeed a letter. Nevertheless, the ".VBS" stood for Visual Basic Script, a program that would run when opened. As not many people knew this, they just opened the letter, ignoring the latter file extension, and unleashed a virus that would cost billions and billions of dollars in lost work hours and information property.[1]

As the sun rose from east to west, more people reported for work and opened their e-mails containing the malicious ILOVEYOU virus. People going through their daily routine of checking their e-mails in the morning were unknowingly and innocently spreading the virus that would later be known as the love bug virus. It spread faster than wildfire. In a matter of hours, the virus had traveled westward, from East Asia, to Europe, and then to America.[2] "The cost worldwide of the first five days of the 'I Love You' bug of spring 2000 reached US$6.7 billion."[3] Indeed, because of its

1. D. Ian Hopper, *Copycat viruses following 'ILOVEYOU' computer bug are no joke*, CNN.COM, May 4, 2000, *available at* http://archives.cnn.com/2000/TECH/computing/05/04/ iloveyou.03/ (last accessed Aug. 19, 2008).

2. D. Ian Hopper, *Authorities may be zeroing in on ILOVEYOU suspect: Philippine Internet provider expects warrant to be served soon*, CNN.COM, May 5, 2000, *available at* http://archives.cnn.com/2000/TECH/computing/05/05/iloveyou.02/index.html (last accessed Aug. 19, 2008) [hereinafter Hopper, *Authorities*].

3. GRAEME R. NEWMAN & RONALD V. CLARKE, SUPERHIGHWAY ROBBERY: PREVENTING E-COMMERCE CRIME 52 (2003).

tremendous effect, computer experts were on the trail of the virus' author right away; not long after, authorities were able to pinpoint the source of the virus as the Philippines. In less than a week, the apartment of the suspected creator of the virus was searched, and soon afterwards, the ingenious perpetrator was in the hands of the authorities. Onel de Guzman was presented to the media in a press conference in Manila as having "accidentally" released the virus.[4] The world had its eyes on the Philippines. The Philippines, however, had no law to prosecute the offender. The most officials could find at the time was a credit card fraud law, the Access Devices Regulation Act of 1998.[5] It is a basic tenet in Philippine law that there is no crime where there is no law that incriminates an act.[6] This is embodied in the maxim "*nullum crimen sine poena, nulla poena sine legis*."[7] Thus, the Philippines had little basis, if any, to prosecute the offender for his misconduct, not because there was a lack of evidence, but because there was a lack of law.

Embarrassing as it was, Philippine legislators immediately took to action and passed Republic Act (R.A.) No. 8792, better known as the e-

4. Maria Ressa & D. Ian Hopper, *Investigator: Dropout may be admitting role in virus attack*, CNN.COM, May 12, 2000 *available at* http://archives.cnn.com/2000/ASIANOW/southeast/ 05/12/ilove.you/ (last accessed Aug. 19, 2008).

5. Raju Chebium, *'Love Bug' suspect could face both civil and criminal trials*, CNN.COM, May 8, 2000 *available at* http://archives.cnn.com/2000/LAW/05/08/love.bug.02/index. html (last accessed Aug. 19, 2008); *see* An Act Regulating the Issuance and Use of Access Devices, Prohibiting Fraudulent Acts Committed Relative Thereto, Providing Penalties and for Other Purposes [Access Devices Regulation Act of 1998], Republic Act No. 8484 (1998).

6. LUIS B. REYES, THE REVISED PENAL CODE: CRIMINAL LAW BOOK ONE (15th ed. 2001) [heinafter REYES, BOOK ONE]; JOAQUIN G. BERNAS, S.J., THE 1987 CONSTITUTION OF THE REPUBLIC OF THE PHILIPPINES: A COMMENTARY 494 (2003 ed.) (citing U.S. v. Luling, 34 Phil. 725, 728 (1916)).

> The State having the right to declare what acts are criminal, within certain well defined limitations, has a right to specify what act or acts shall constitute a crime, as well as what proof shall constitute prima facie evidence of guilt, and then to put upon the defendant the burden of showing that such act or acts are innocent and are not committed with any criminal intent or intention.

7. RUBEN E. AGPALO, STATUTORY CONSTRUCTION 473 (5th ed. 2003). Translated, the maxim means "*There is no crime without a penalty, and there is no penalty without a law.*"

Commerce Act of 2000.[8] As it was though, it was too late to prosecute Onel de Guzman as R.A. No. 8792's penal provisions could not be given retroactive effect.[9]

It has been a little over eight years since the love bug virus placed the Philippines in the world's limelight. Indeed, the e-Commerce Act of 2000 has since then been enacted and could now be used to prosecute cyber offenders. Nevertheless, cybercrime continues to evolve and continues to grow. As the world of computers and the Internet is very dynamic, the means and methods of cyber offenders evolve and become more complex. Computer crime may very be only at its infancy, but the Philippines cannot wait for another love bug before it ensures that its laws are sufficient to deal with cyberattacks, lest it place itself in the same embarrassing and shameful situation. Computer crimes could have evolved such that the means, methods, and acts used to carry them out could no longer be covered by the e-Commerce Act of 2000. It must be stressed that *nullum crimen sine poena, nulla poena sine legis*.

It is important to question the sufficiency of the e-Commerce Act of 2000 and other pertinent laws as cybercrime is known to be increasing. A 2003 report by an American-based computer threat monitoring company provided that "network-based Internet attacks rose by 19 percent in the first [six] months of 2003. … On average, companies reportedly experienced about thirty-eight attacks per week in the first half of 2003, up from thirty-two per week just a year before."[10] *Cyberlaw: Text and Cases* aptly provides:

> The lessons … have not been lost on criminals or on law enforcement efforts. The means of committing crimes are now cheap and ubiquitous. A computer with an Internet connection is all that is needed. Moreover, the number of potential victims is, in theory, limited by only one factor — the number of users connected to the Internet. It is clearly more efficient to perpetrate crime in cyberspace than in the physical world.[11]

The same book uses the analogy of locks which, from the time of its invention, has been picked by criminals, and continues to be so up to the

---

8. Susan W. Brenner, Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law, *available at* http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82.html (last accessed Aug. 19, 2008).

9. PHIL. CONST. art. III, § 22 (which provides, "No ex-post facto law or bill of attainder shall be enacted."). *See* Brenner, *supra* note 8.

10. BERNADETTE H. SCHELL & CLEMENS MARTIN, CYBERCRIME 28 (2004).

11. GERALD R. FERRERA, ET AL., CYBERLAW TEXT AND CASES 407 (2d ed. 2004).

present age.[12] It further provides that the Federal Bureau of Investigation of the United States believes that computer criminals will be the next significant wave of crime perpetrators.[13] The authors state:

> It is helpful to add some numbers to the discussion as a way of explaining the depth and breadth of the problem facing both governments and businesses. Just in one month, June 2002, the Department of Justice (of the United States of America) handled a number of cases, ranging from trafficking in counterfeit Microsoft software, stealing trade secrets from a Harvard biology lab, malicious spamming, selling fake Derek Jeter and Nomar Garciaparra sports memorabilia on eBay, credit card scams, to selling prescription drugs online. Half of Visa International, Inc.'s transactions from online sales were disputed or full-fledged frauds. In 1999, federal agents investigated a credit card billing scam. One man alone engineered $45 million of charges in hundreds of thousands of fraudulent transactions. More than 25 percent of all Fortune 500 corporations have been victimized by computer crime.[14]

Thus, it can be seen that computer crime is not only here to stay, but is growing. It has been said that, "as more novices connect to the Internet, there becomes an overall declining expertise of users. These represent ever-greater vulnerabilities."[15]

*B. Significance of the Study*

As can be gleaned above, computer crime is growing. The Philippines has once been placed in a humiliating situation where billions of dollars were lost around the world, and yet it could not hold anyone legally accountable because of the lack of pertinent laws, or at least, a law to deal with such a cyberoffender. When computer frauds were discovered in the earlier days, people hardly paid attention. Some poorly drafted computer crime laws were passed in the hopes that those would be enough. Yet, today, the world still faces an ever growing number of computer crimes.[16] The harsh reality is that with progress and new inventions come new crimes or ways of committing them. Many of the world's developed countries have accepted this reality and continually update and upgrade their laws. Europe, for instance, has recently convened as a body to formulate computer crime legislation. They

12. *Id.*

13. *Id.*

14. *Id.*

15. *Id.*

16. G. JACK BOLOGNA & PAUL SHAW, AVOIDING CYBER FRAUD IN SMALL BUSINESSES 3 (2000).

have found it significant enough to not only have individual state legislation, but to have a convention on cybercrime, perhaps realizing the potential of cybercrime and the need for better and more cooperative legislation to prevent them. It is thus provided in the Preamble of their convention, the Convention on Cybercrime:

> Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation;
>
> Conscious of the profound changes brought by the digitalisation, convergence and continuing globalisation of computer networks;
>
> Concerned by the risk that computer networks and electronic information may also be used for committing criminal offences and that evidence relating to such offences may be stored and transferred by these networks;[17]

Whereas Europe has found it significant enough to not only formulate a cybercrime law but to convene for the purpose of international cooperation, the Philippines' own version, the e-Commerce Act of 2000, is hardly focused on the criminal aspect, but rather on the commercial aspect of cyber legislation. The e-Commerce Act of 2000 really only has one section dedicated to penalizing cyber offenders, interestingly found in its Final Provisions part.[18]

It should further be noted that the need for cybercrime legislation is not merely a matter of good policy, but rather a necessity because of the ever growing reliance of society on computers. It is a well-known fact that, today, banks, stock exchanges, transportation systems such as airlines, and even retail stores using point-of-sales systems rely heavily on computers. Cyberattacks on the computer systems of these facilities could cause serious economic sabotage. Dr. Dorothy Denning, a cybercrime expert from Georgetown University, stated that "the potential for destabilizing a civilized society through cyberattacks against banking or telecommunications systems, for example, becomes increasingly large."[19] In the Philippines, the National Statistics Office, in a 2002 survey updated on December 2003, provided that

17. Convention on Cybercrime, Nov. 23, 2001, Preamble, ETS No. 185 (2001) (emphasis supplied).

18. 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 [e-Commerce Act of 2000], Republic Act No. 8792, § 33 (2000). *See* 3 RECORD OF THE SENATE 731, S. 1902, 11th Cong., 2d Sess. (Mar. 21, 2000).

19. SCHELL & MARTIN, *supra* note 10, at 14.

most industries have a high usage of information and communication technology (ICT). Notable among these industries were the financial intermediation industry at 96.6%; the electricity, gas, and water industry at 93.2%; and the health and social work industry at 92%. The industries with the least ICT usage are the agriculture, fishing, and mining and quarrying industries.[20] The same survey showed that the financial intermediation industry had the highest number of personal computers per establishment.[21] Placed together with Internet access rate — the proportion of the number of internet users to the total number of personal computer users — the financial intermediation industry still ranked high at 76%. Other personal, community, and social services also ranked high at 81%.[22] This summary of figures as provided by the Industry and Trade Statistics Department of the National Statistics Office shows that the Philippines is highly reliant on information technology. The high usage of information technology in many industries means that the potential for damage in the country by cyber offenders is great.

The Philippines cannot be oblivious to crimes perpetrated through computers. Indeed, the Philippines may not be as developed as other countries, but this does not mean that it is devoid of computers or the Internet. The National Statistics Office, in its publication *Philippines in Figures 2006*, provided that the estimated number of subscribers to Internet service in the Philippines has been increasing. From 800,000 in 2002, the number of Internet subscribers increased to 1,200,000 in 2004.[23] Although this number may seem small, one must keep in mind that one subscription may have more than one user. A testament to the participation of the Philippines in the global community of computer networks, albeit in a negative light, is Onel de Guzman's 'ILOVEYOU' virus.[24] The Philippines may not, as yet, be part of any cybercrime convention. As a member of the global community, however, it has to fill its own void and have its own legislation to prevent different forms of cybercrime or, at least, to penalize

20. National Statistics Office, 2002 Survey of Information and Communication Technology (SICT) of Philippine Business and Industry, *available at* http://www.census.gov.ph/data/sectordata/sr0373tx.html (last accessed Aug. 19, 2008).

21. *Id.*

22. *Id.*

23. NATIONAL STATISTICS OFFICE, PHILIPPINES IN FIGURES 2006 10 (2006), *available at* http://www.census.gov.ph/data/publications/PIF2006.pdf (last accessed Aug. 19, 2008).

24. Hopper, *Authorities*, *supra* note 2.

cyber offenders.[25] More than just avoiding being in a shameful situation, this need for legislation partakes of the nature of a responsibility to the global community in global progress — cyber progress at that.

### *C. An Overview of the Study*

This Note is concerned with cybercrime[26] and the sufficiency of Philippine laws to combat cybercrime. Particular attention was given to the e-Commerce Act of 2000, the Revised Penal Code,[27] and other penal laws pertinent to the cybercrime being considered. The particular cybercrimes analyzed in this Note are phishing, denial of service, and cyberstalking. These crimes have particularly been given less attention in the Philippines than the common cybercrimes of hacking and dissemination of viruses.

This Note does not delve into the need for international cybercrime legislation, but concentrates rather on Philippine legislation. Further, matters of jurisdiction are not extensively discussed, as it is assumed that the cyber offender will be from the Philippines, thus violating Philippine laws. As criminal law is jurisdictional, the primary focus of this Note is on the territorial jurisdiction of the Philippines.

The nature and essence of cybercrimes is first examined by this Note to better understand these crimes. From this, the elements of the offenses of phishing, denial of services attacks, and cyberstalking are ascertained. Due to the lack of jurisprudence on the matter however, a determination of the insufficiency of Philippine laws vis-à-vis these offenses is made by applying their elements to various laws that may find applicability. Ultimately, the insufficiency of Philippine laws against cybercrime is determined by whether or not the cyber offenders of the cybercrimes studied could be prosecuted under Philippine laws.

After making this determination, foreign laws are examined to see how some developed countries have formulated their laws to deal with these cybercrimes.

## II. CYBERCRIME

It is perhaps tragic that a tool such as the Internet, developed for the military and subsequently used for societal progress and commerce, can easily be turned around to further vile agendas. Tragic as it may be, perhaps that

25. Brenner, *supra* note 8.

26. Cybercrime and cyberoffenses are used interchangeably throughout this Note.

27. An Act Revising the Penal Code and Other Penal Laws [REVISED PENAL CODE], Act No. 3815 (1932).

simply is how reality will always be — so long as there is wealth to steal and people to fool, there will always be those who steal and fool. Sadly, the cyber world has not escaped this reality.

*A. An Outlook on Cybercrime*

The idea of cybercrime was probably born in the minds of would-be cyber criminals as early as they realized that computers stored something of value — information.[28] Perhaps this idea was not as enticing as it is now, considering much of the information available before were scientific data that required scientific analysis and were of little monetary value. As commercial use of the Internet grew, however, more and more information could be acquired to obtain financial gain. It was not long before credit card transactions were being made online, and money was being transferred via computer networks.[29]

The early age of computer crime was different, as access to computers and to networks was difficult. Personal computers were hardly known and there were no "user-friendly" applications.[30] Computers then were expensive and would usually take up an entire room. Furthermore, "working with early systems required the ability to 'speak' *machine language* — that is, to communicate in the 1s and 0s of binary calculation that computers understood."[31] Gradually, computing became easier and less expensive and, with this, the cybercrime problem emerged.[32] Today, a great mass of people worldwide have access to computers and to the Internet. Even people who do not own computers can go to an Internet café, a public library, or a school for computer access.[33]

During the time of ARPANET,[34] security was a concern for the military and, at the same time, a non-issue to research scientists who were more interested in the potential of the technology. In 1988, a worm was released

28. DEBRA LITTLEJOHN SHINDER & ED TITTEL, SCENE OF THE CYBERCRIME: COMPUTER FORENSICS HANDBOOK 50 (2006).

29. DAVID I. BAINBRIDGE, INTRODUCTION TO COMPUTER LAW 291 (2000).

30. SHINDER & TITTEL, *supra* note 28, at 2.

31. *Id.*

32. *Id.*

33. *Id.*

34. The early version of the Internet developed by the Department of Defense of the United States of America. *See generally* Dave Kristula, The History of the Internet, *available at* http://www.davesite.com/webstation/net-history.shtml (last accessed Aug. 19, 2008).

which spread across the United States and infected thousands of computers. This resulted in a shutdown of a large portion of the Internet and woke Internet users to the stark reality that not everyone shared their idealism on the use of the Internet.[35] By no means was this worm — a cybercrime — the last.

During the 1990s, Internet security became more and more of an issue, especially with the commercialization of the Internet and the ease of access to computers and to software applications that may be used for cybercrime. Determining whether the concern came ahead of cybercrimes or cybercrimes ahead of the concern would be like a *chicken-or-the-egg* chase. Regardless of which came first, the truth was that cybercrime was rising. Among the cybercrimes committed were hacks to different websites and networks, including that of the United States Central Intelligence Agency, the United States Department of Commerce, eBay, and the New York Times.[36] There was also the Melissa virus which caused e-mail servers to shut down. There was a fraudulent website made to appear as if it were an authentic Bloomberg financial story that caused the shares of a small technology company to rise 31% because of the false news.[37]

The dawn of the new millennium brought about the commission of more cybercrime, including the infamous love bug virus made by a Filipino, and denial of service attacks on website giants such as Yahoo! and Amazon.[38] "From the infamous 'Nigerian letter' scam to the use of the Net to plot the September 11, 2001 terrorist attacks, crime was running rampant on the network — and still is today."[39]

### *B. Types of Cybercrime*

Several types of cybercrime have emerged since the beginnings of computers and computer networking. Spawned by the creativity of the human mind together with the gradual increase of access to and the ease in the use of computers, various forms of cybercrime have been reported and identified. Some are new ways of committing old crimes with computers used merely as conduits or to facilitate their commission, while others are original in the sense that they could not be committed without computers and computer

35. SHINDER & TITTEL, *supra* note 28, at 61.

36. *Id.* at 62.

37. *Id.*

38. *Id.*

39. *Id.*

networking.[40] Some of the more prevalent and well-known forms of cybercrime are hacking and cracking, viruses and worms, and piracy. Nevertheless, by no means are cybercrimes limited to these well-known forms. In fact, there is a whole gamut of activities that can be classified as cybercrime. While some have been considered by law one way or another by various countries, others are simply overlooked. Other forms of cybercrime include child pornography,[41] password sniffing,[42] Trojan horses,[43] and even cyberterrorism.[44]

While the focus of this Note is on the not so prevalent and well-known — hence less treated by laws, while equally potentially damaging — forms of cybercrime, a brief background is given on hacking and cracking and viruses for a better understanding of the matter, especially since these cybercrimes are particularly mentioned by the e-Commerce Act of 2000.[45] From there, the Note moves on to its main focus — phishing and identity theft, denial of service, and cyberstalking.

1. Hacking and Cracking

The subjects of various movies, hacking and cracking have constantly been brought to the limelight, and are perhaps the more popular forms of cybercrime. The movies usually portray them as a manner of gaining access to a computer network or system via a remote computer, usually that of a government agency, and stealing or altering valuable information. Beyond the fictional stories of movies though, they are a reality that governments have accepted and considered, particularly when drafting their laws. The Philippine e-Commerce Act of 2000 takes particular notice of hacking and cracking under Section 33.[46]

Hacking and cracking are similar, the difference being that cracking is the name usually given to a malicious form of hacking.[47] The distinction is not always clear, however, and both terms are sometimes used interchangeably. The e-Commerce Act of 2000 in fact does not make any

40. BAINBRIDGE, *supra* note 29, at 285.

41. FERRERA, ET AL., *supra* note 11, at 416-18.

42. *Id.* at 425.

43. *Id.*

44. *Id.* at 433-35.

45. e-Commerce Act of 2000, § 33.

46. *Id.*

47. FERRERA, ET AL., *supra* note 11, at 424.

distinction, and defines them as one.[48] Under Section 33, it defines hacking or cracking as follows:

> 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.[49]

Hacking is also more simply defined as "the accessing of a computer system without the express or implied permission of the owner of that computer system."[50] Cases of hacking and cracking have been rampant in the recent years.[51] Hacking is not inherently malicious or criminal in itself. It is more often considered as a form of mental challenge for hackers, in which they attempt to overcome the security of certain networks to prove themselves as well as the vulnerability of supposedly secure networks. They are often harmless, and no financial or other form of gain is made, and the motivation is usually that of a sense of achievement.[52] If anything, they are nuisances for the most part to system managers or network administrators.

Cracking, on the other hand, is the sinister side of hacking and involves ominous intent.[53] They are not done simply for prestige or a sense of achievement. They involve financial, property, or moral damage. Although cracking also involves unauthorized access to a computer system without the

48. e-Commerce Act of 2000, § 33. During the deliberations in the Senate of Senate Bill 1902 (which later became the e-Commerce Act of 2000), Senator Tatad attempted to prevent the word "hacking" from appearing in the law. He tried to convince his colleagues that hacking is not a crime, as opposed to cracking. 3 RECORD OF THE SENATE 731-33, S. 1902, 11th Cong., 2d Sess. (Mar. 21, 2000).

49. e-Commerce Act of 2000, § 33 (a) (emphasis supplied).

50. BAINBRIDGE, *supra* note 29, at 307.

51. FERRERA, ET AL., *supra* note 11, at 424.

52. BAINBRIDGE, *supra* note 29, at 307.

53. FERRERA, ET AL., *supra* note 11, at 424.

permission of the owner of the computer system, as opposed to hacking, here there is malicious intent.[54]

2. Viruses and Worms

Viruses and worms are other common and notorious forms of cybercrime. Every so often, people receive news warning about a virus that is quickly spreading. There are also cases wherein news is received after the virus has spread and has done its damage, as in the case of the love bug virus. Some viruses are mere nuisances, much like the common cold, while other viruses are more potentially destructive, more like the bird flu (H5N1 virus) or the human immunodeficiency virus (HIV). Needless to say, computer viruses are named as such due to their similarity to biological viruses.

There are many various definitions of viruses, although they essentially refer to the same thing. The dictionary definition of a virus is that it is "a computer program usually hidden within another seemingly innocuous program that produces copies of itself and inserts them into other programs and that usually performs a malicious action (as destroying data)."[55] Worms are very similar to viruses, the difference being that worms require a computer network to replicate itself, while a virus may be spread through other means such as through diskettes or flash drives. A worm is defined as "a usually small self-contained computer program that invades computers on a network and usually performs a malicious action."[56]

Viruses are specifically treated by the e-Commerce Act of 2000. It provides thus:

> 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.[57]

54. *Id.*

55. MERRIAM-WEBSTER DICTIONARY ONLINE, *available at* http://www.merriam-webster.com/dictionary/virus (last accessed Aug. 19, 2008).

56. MERRIAM-WEBSTER DICTIONARY ONLINE, *available at* http://www.merriam-webster.com/dictionary/worm (last accessed Aug. 19, 2008).

57. e-Commerce Act of 2000, § 33 (a) (emphasis supplied).

A thorough study on viruses, as well as this provision of the law, however, led to the conclusion that the said provision, as well as the e-Commerce Act of 2000, was inadequate to define and penalize the crime of disseminating a virus. The author indicated that the said law did not exhaustively consider the nature of viruses, and further, its fault was that it "indiscriminately lumped" the crime of disseminating viruses with hacking or cracking.[58] She further proposed a separate law to supplement the e-Commerce Act in penalizing the dissemination of viruses.[59]

3. Identity Theft and Phishing

There seems to be a lack of awareness of identity theft in the Philippines, perhaps because it is not as rampant in the Philippines as in other countries, or perhaps because Filipinos are more careful with their credit cards and are wary about online transactions. Although identity theft is occurring at an alarming rate in the United States, for example, there is still some "false sense of security that this is not going to happen in the Philippines because 'we are not yet as sophisticated.'"[60] Whatever may be the reason, however, identity theft is on the rise in the Philippines. In 2002, for example, warehouse club operator Pricesmart, Inc. had to deal with more than a colossal one billion pesos' worth of fraudulent credit card transactions in their Congressional Avenue branch in Quezon City.[61] Metrobank recently warned its depositors of phishing attempts.[62]

58. Deanna M.S. Lorenzo, Virus: A Lethal Epidemic — Is the E-Commerce Act Enough? 39 (2002) (unpublished J.D. thesis, Ateneo de Manila University) (on file with the Professional Schools Library, Ateneo de Manila University).

59. *Id.* at 39-43 & 68-73.

60. Maria Salve Duplito, *Identity theft on the rise in Manila*, MANILA STANDARD TODAY, Mar. 25, 2004 *available at* http://money.inquirer.net/personalfinance/printable_personalfinance.php?yyyy=2004&mon=03&dd=25&file=1 (last accessed June 21, 2008).

61. *Id.*

62. *Metrobank warns depositors about 'phishing' attempts*, MANILA STANDARD TODAY, May 15, 2006 *available at* http://www.manilastandardtoday.com/?page=interactive01_may15_2006 (last accessed June 21, 2008).

*a. Identity Theft*

"'Identity theft' is a term referring to a variety of crimes, all of which involve 'stealing' someone's personally identifying information."[63] Various methods may be used to acquire 'personally identifying information,' the latest variant being that of using the Internet.[64] Identity theft though usually starts with one's misuse of personally identifying information.[65] A simple mishandling of personal information, such as losing a credit card or throwing away billing statements may lead to identity theft. Other times, identity thieves are more deliberate in stealing personal information, such as stealing one's wallets or diverting billing statements. The following are some of the known methods of identity thieves in stealing such information:

> Phishing – The identity thief (thieves) pretend(s) to be financial institutions or companies, and send spam e-mail or pop-up messages to trick one to reveal his or her personal information.
>
> Dumpster Diving – Rummaging through trash looking for bills or other papers with one's personal information.
>
> Skimming – Stealing credit/debit card numbers by using a special storage device while one's card is being processed (as in during a purchase).
>
> Changing addresses – Diverting billing statements to another location by completing a change address form.
>
> Old-Fashioned Stealing – Stealing wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They may also steal personnel records, or bribe employees who have access to such records.
>
> Pretexting – Using false pretenses to obtain one's personal information from financial institutions, telephone companies, and other sources.[66]

Once the identity thief has acquired the necessary information, he or she can make transactions — such as transferring money from bank accounts, incurring debts, or even committing crimes — posing as his or her victim.[67]

---

63. Holly K. Towle, *Identity Theft: Myths, Methods, and New Law*, 30 RUTGERS COMPUTER & TECH. L.J. 237, 241 (2004).

64. *Id.* at 238.

65. Federal Trade Commission, Fighting Back Against Identity Theft, About Identity Theft, *available at* http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/about-identity-theft.html (last accessed Aug. 19, 2008).

66. *Id.*; FEDERAL TRADE COMMISSION, ID THEFT: WHAT IT'S ALL ABOUT 2 – 3 (2005), *available at* http://www.ftc.gov/bcp/conline/pubs/credit/idtheftmini.pdf (last accessed Aug. 19, 2008).

This Note delves into phishing, as this is the form of identity theft that concerns cybercrime. While much identity information is stolen in the physical world, "the Internet has the potential to become a primary resource for fraudsters to steal identities."[68] It can be used to perpetrate scams to deceive unknowing individuals into sharing sensitive personal and financial information.[69]

*b. Phishing*

Phishing is a recent trend on how identity thieves steal personal information. The term was coined by hackers in the mid-1990s to refer to the art of stealing AmericaOnline accounts.[70] A definition given in a Report to the Minister of Public Safety and Emergency Preparedness of Canada and the Attorney General of the United States is that it is the "creation and use by criminals of e-mails and websites — designed to look like they come from well-known, legitimate and trusted businesses, financial institutions and government agencies — in an attempt to gather personal, financial and sensitive information."[71] Another definition given by the Anti-Phishing Working Group (APWG), a multinational industry coalition that focuses on phishing,[72] is that it is "a form of online identity theft that employs both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials."[73] Through phishing, identity thieves are able to trick gullible users — often through social engineering — into thinking that they are giving or sending their personal information to authentic and legitimate sites that would need the said personal information. The truth of the matter is that those sites are fake and the acquired

67. Towle, *supra* note 63, at 243.

68. *Id.* at 248.

69. *Id.*

70. Andrew Abraham, *The Regulation of Virtual Banks: A Study of the Hong Kong Perspective,* 10 NO. 12 J. INTERNET L. 3, 9 (2007).

71. BINATIONAL WORKING GROUP ON CROSS-BORDER MASS MARKETING FRAUD, REPORT ON PHISHING: A REPORT TO THE MINISTER OF PUBLIC SAFETY AND EMERGENCY PREPAREDNESS CANADA AND THE ATTORNEY GENERAL OF THE UNITED STATES 4 (2006), *available at* http://www.usdoj.gov/opa/report_on_phishing.pdf (last accessed June 21, 2008) [hereinafter BINATIONAL WORKING GROUP].

72. *Id.* at 5.

73. ANTI-PHISHING WORKING GROUP (APWG), PHISHING ACTIVITY TRENDS: REPORT FOR THE MONTH OF FEBRUARY, at 1 2007, *available at* http://www.antiphishing.org/reports/apwg_report_february_2007.pdf (last accessed Aug. 19, 2008) [hereinafter APWG, PHISHING ACTIVITY TRENDS].

information can then be used by the identity thieves to defraud companies under the identities of their victims or can be sold to others willing to do the same. "Often 'phishers' will sell credit card or account numbers to other criminals, turning a very high profit for a relatively small technological investment."[74]

In a report published by the APWG, phishing rose in 2006 and even reached a record high of 29,930 unique reports for the month of January 2007.[75] According to the same study, 135 brands were hijacked during the month of February 2007.[76] It was also determined, unsurprisingly, that the most targeted industry sector for phishing is financial services, accounting for 92.6% of all attacks for the same period. Retail stores, Internet service providers, and other sectors were also targeted, albeit to a much lesser degree.[77] From July 2004 to March 2005, phishing attempts increased 28% each month.[78]

*c. Stages of Phishing*

A typical phishing scheme starts with the phisher creating replicas of an authentic website, e-mail, or both, carrying the logo and other intricacies of the brand (target brand), which they intend to deceive their victims with. Such brands are more often than not of financial institutions.[79] These websites and e-mails can look very authentic and can, thus, be very deceptive.[80] Furthermore, they ask for or require personal information to be given, such as, but not limited to, login names, passwords, account numbers, birthdays, and other personally identifying information. Subsequently, these replica or fake e-mails are sent to as many users as possible. The e-mails may ask the victim to either send their personal information to a certain e-mail address that seemingly belongs to the target brand company, or the e-mails

74. BINATIONAL WORKING GROUP, *supra* note 71, at 5.

75. APWG, Phishing Activity Trends, *supra* note 73 (The Phishing Attack Trends Report is published monthly by the Anti-Phishing Working Group, an industry association focused on eliminating the identity theft and fraud that result from the growing problem of phishing and e-mail spoofing.).

76. *Id.*

77. *Id.*

78. *Internet Crime Complaint Center: New trend identified among Phishing targets*, 5 NO. 13 CYBERCRIME L.REP. 12 (2005).

79. BINATIONAL WORKING GROUP, *supra* note 71, at 7.

80. *See generally* Anti-Phishing Working Group (APWG), Phishing Archive, *available at* http://www.antiphishing.org/phishing_archive/phishing_archive.html (last accessed Aug. 19, 2008) [hereinafter APWG, Phishing Archive].

may direct the victim to a replica website through a link, wherein they could enter their personal information, at times, ironically, in the belief of protecting their personal information.[81] Hence, a victim may, for example, receive an e-mail supposedly from his or her bank requiring her to give personal information or else her bank account might be compromised.

Three usual elements are employed by phishers to dupe their victims. The first one is by using familiar corporate trademarks or tradenames, logos, and other marks commonly associated with the target brand being used to deceive. Thus, a potential victim could receive an e-mail from his or her bank, such as Equitable-PCI Bank or Bank of the Philippine Islands, together with the corresponding logo of these banks, asking him or her to provide the sender with important personal information. This element can be a very effective technique, as these corporate trademarks are familiar to Internet users who could possibly trust these e-mails bearing the said logos.[82] The second element is by causing the potential victim to worry or have a sense of urgency. This social engineering technique is accomplished by e-mails containing warnings that if the potential victim does not follow instructions, certain negative consequences may happen, such as account terminations, penalties, fees, or, ironically, a breach of their account security or privacy. This impairs the judgment of the potential victim, as instead of being wary, he or she becomes concerned or worried, possibly even afraid.[83] The third element is by taking advantage of the lack of technical knowledge of many users in determining the authenticity of the said e-mails, compounded by the lack of adequate tools to authenticate the said e-mails.[84]

Summarized, the elements of phishing are as follows:

(a) That an offender solicits, requests, or otherwise induces another to provide personally identifying information

(b) That such was done through the creation of an electronic mail message, website, or otherwise through the Internet

81. BINATIONAL WORKING GROUP, *supra* note 71, at 7; Iconix, Inc. v. Tokuda 457 F.Supp.2d 969, 973 (2006); Associated Bank-Corp. v. Earthlink, Inc., 2005 WL 2240952 1 (W.D.Wis. 2005).

82. BINATIONAL WORKING GROUP, *supra* note 71, at 7.

83. *Id.*

84. *Id.* at 8. *See generally* APWG, Phishing Archive, *supra* note 80.

> (c) That such was made without right or authority to request or solicit such personally identifying information, or otherwise through false representation.[85]

4. Denial of Service Attacks

*a. Overview of Denial of Service Attacks*

Denial of Service is a form of cybercrime wherein — through some manipulation — one prevents another from using the Internet or some other online based service. Thus, a person may be prevented from accessing his or her e-mail or Internet services, or a website itself may be prevented from being accessed. This may be done by flooding a network with traffic or by disrupting connections.[86] The White House website, as well as the websites of Amazon, Yahoo, Dell, eBay, and CNN, for example, have been affected by denial of service attacks.[87]

More formally, a denial of service attack is defined by the Computer Emergency Response Team (CERT)[88] as follows:

> A "denial of service" attack is characterized by an explicit attempt by attackers to prevent legitimate users of a service from using that service. Examples include:

85. GREGG TALLY, ET AL., ANTI-PHISHING: BEST PRACTICES FOR INSTITUTIONS AND CONSUMERS 3 (2004), *available at* http://www.antiphishing.org/sponsors_technical_papers/AntiPhishing_Best_Practices_for_Institutions_Consumer0904.pdf (last accessed Aug. 19, 2008).

86. FERRERA, ET AL., *supra* note 11, at 425.

87. *Id.*

88. The CERT Program is part of the Software Engineering Institute (SEI), a United States federally-funded research and development center at Carnegie Mellon University in Pittsburgh, Pennsylvania. Following the Morris worm incident, which brought 10 percent of internet systems to a halt in Nov. 1988, the Defense Advanced Research Projects Agency (DARPA) charged the SEI with setting up a center to coordinate communication among experts during security emergencies and to help prevent future incidents. This center was named the CERT Coordination Center (CERT/CC).

One of the primary objectives of CERT is to analyze the state of Internet security and convey that information to the Internet community. The CERT/CC monitors public sources of vulnerability information and regularly receives reports of vulnerabilities. After analyzing the potential vulnerabilities, experts from CERT inform technology producers and work with them to facilitate their response to problems.

- Attempts to "flood" a network, thereby preventing legitimate network traffic
- Attempts to disrupt connections between two machines, thereby preventing access to a service
- Attempts to prevent a particular individual from accessing a service
- Attempts to disrupt service to a specific system or person.[89]

The main objective of the cyber offender or the denial of service attacker is to disable computer network connectivity. This could potentially be damaging, particularly to services or industries or organizations that rely heavily on computer networking (i.e. the Internet).[90] Thus, Amazon, whose main business is selling books and other items online, or eBay, an online auction and commerce site, could severely be affected by a denial of service attack. If service is denied to their websites, they would not be able to generate income. The same may happen to financial services sites, such as BPITrade, which derives income from commissions from stock trading made through its website.[91] Furthermore, denial of service attacks may also disrupt communications within organizations (especially multinational organizations) that rely on the Internet (i.e. e-mail or instant messaging) as a cheap alternative to voice or other traditional methods of communication. "Denial of service attacks can result in significant loss of time and money for many organizations."[92]

*b. Stages of Denial of Service Attacks*

A denial of service attack is often committed by consuming scarce computer and networking resources, such as by flooding a network to slow down or even prevent network traffic.[93] There are many technical ways of consuming these scarce resources, but the objective remains the same — to prevent legitimate users from using an online service.

One technical way of conducting a denial of service attack is by preventing computers or networks from communicating with the main

89. CERT, Denial of Service Attacks, *available at* http://www.cert.org/tech_tips/denial_of_service.html (last accessed Aug. 19, 2008).

90. *Id.*

91. *See generally* BPI Trade, http://www.bpitrade.com (last accessed Aug. 19, 2008); BPI Trade, http://www.bpitrade.com/learnmoreload.asp (last accessed Aug. 19, 2000).

92. CERT, *supra* note 89.

93. *Id.*

network. This is done by establishing a connection with the victim machine, and preventing the ultimate completion of that connection.[94] In other terms, this is like making a phone call to a law or airline office which cannot be terminated by the receiver (i.e. the office). As long as the phone call is active, the office cannot make any outgoing calls, nor receive other incoming calls. The telephone line pertaining to that specific telephone number will be tied-up and rendered useless. If the office only has five telephone numbers, and receives multiple phone calls every hour, it will definitely be harder to contact that office and for the office to contact others. Now, if three of the five telephone numbers were rendered useless, clients of the law office, or customers wanting to buy a plane ticket will be frustrated. If all five phone lines were rendered useless, the law or airline office would lose valuable clients. Computer networks function in a similar way.

Another technical way of conducting a denial of service is attack is by consuming all the available bandwidth of a network by generating a large number of packets directed to a network.[95] Bandwidth is the amount of data that can be transferred from one computer or network to another.[96] Imagine bandwidth as a highway and packets as cars. A single car on a highway could travel really fast. The more cars there are in the highway, however, the slower traffic becomes. If several cars are made to go to a single destination at the same time, the highway will be clogged, causing a jam or slow down that could prevent cars from reaching their destination. The same effect can happen over the information highway, particularly when a person deliberately sends packets to a single network or computer designed to overload such network or computer.

One other form of denial of service attack is when the attacker changes or destroys the configuration information of a computer or network in order to prevent a user from accessing the main network or the Internet.[97] Computers and networks are composed of addresses and configurations that allow them to communicate with each other, much like a postal service makes use of zip codes, country codes, area codes, and other tools to facilitate the sending of snail mail. If these addresses and configurations are changed, electronic data messages will not reach their correct destinations, much like how snail mail will not reach its correct destinations if the zip

94. *Id.*

95. *Id.*

96. MERRIAM-WEBSTER DICTIONARY ONLINE, *available at* http://www.merriam-webster.com/dictionary/bandwidth (last accessed Aug. 19, 2008) (the capacity for data transfer of an electronic communications system).

97. CERT, *supra* note 89.

codes and country codes were all jumbled up. Thus, if one maliciously alters or destroys these configuration information, it would be tantamount to preventing a user from accessing a network.

It was indicated in a recent report that a simple denial of service attack could cripple up to 85% of the Internet.[98]

As can be gleaned above, the elements of denial of service attacks involve:

> (a) The intentional unauthorized access, interference, or disruption of a computer or an electronic communication device or online service; or
>
> (b) the intentional unauthorized consumption of computer network resources; or
>
> (c) the intentional unauthorized alteration of the configuration information of a computer or electronic communication device
>
> (d) in order to hinder or prevent legitimate access to or of a computer or network or online service.

5. Cyberstalking

Although stalking has probably been there longer, it is only recently that it has been legally recognized.[99] Though even this legal recognition may have failed to take into account the cyber version of stalking — cyberstalking. Be that as it may, cyberstalking is a reality that exists, though exact numbers and statistics are hard to come by. A volunteer organization — Working to Halt Online Abuse (WHOA) — was in fact founded in 1997 to help combat online harassment.[100] Beginning in 2000, they were able to gather statistics based on information given to them by victims, although this data is not

98. *Simple Attack could Cripple Much of Net*, 8 NO. 5 E-COMMERCE L. REP. 15 (2006).

99. Wayne Petherick, Cyber-Stalking: Obsessional Pursuit and the Digital Criminal, *available at* http://www.crimelibrary.com/criminalmind/psychology/cyberstalking/ (last accessed Aug. 19, 2008).

100. Working to Halt Online Abuse (WHOA) is based in York, Maine in the United States. Its current president is Jayne A. Hitchcock, an internationally recognized cybercrime expert. She is a consultant with the Department of Justice Office for Victims of Crime of the United States, as well as the National Center for Victims of Crime. She is the author of eight books, including *Net Crimes and Misdemeanors 2nd Edition: Outmaneuvering Web Spammers, Stalkers, and Con Artists*.

based on the total number of cases they handled. Based on their data, victims were, more often than not, female (73.5%), and stalkers more often than not male (51.5%). Many of the victims were from 18 to 30 years of age (46.5%), followed by those from 31 to 40 years old (27.5%).[101] Another study found that cyberstalking is on the rise. In a 2003 poll, it was determined that one in six office workers in the United Kingdom has been harassed by e-mail.[102]

*a. Definition of Cyberstalking*

Real-world stalking is often characterized by obsession on the part of the stalker. This can drive them to extremes, which may make them dangerous.[103] In the Philippines, stalking has been recognized under R.A. No. 9262, or the Anti-Violence Against Women and their Children Act of 2004.[104] It defines stalking as "an intentional act committed by a person who, knowingly and without lawful justification follows the woman or her child, or places the woman or her child under surveillance directly or indirectly, or a combination thereof."[105]

Cyberstalking is conducted in a similar manner as stalking in the physical world.[106] Offenders may even combine cyberstalking with the more traditional forms of stalking, such as calling the victim's home and following the victim.[107] One definition of cyberstalking is that it "consists of terrorizing people over the Internet and includes communications of taunts, profanity, or demands."[108] Another definition is that it "occurs when an

101. WHOA Comparison Statistics 2000-2006, *available at* http://www.haltabuse.org/resources/stats/Cumulative2000-2006.pdf (last accessed May 7, 2007).

102. Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2 (2004) (citing *E-mail bullying on the rise*, BBC NEWS, Mar. 31, 2003, *available at* http://news.bbc.co.uk/2/hi/technology/2902777.stm (last accessed Aug. 19, 2008)).

103. EOGHAN CASEY, DIGITAL EVIDENCE AND COMPUTER CRIME 601 (2d ed. 2004).

104. An Act Defining Violence against Women and their Children, Providing for Protective Measures for Victims, Prescribing Penalties therefore, and for Other Purposes [Anti-Violence Against Women and Children Act of 2004], Republic Act No. 9262 (2004).

105. *Id.* § 3 (d).

106. CASEY, *supra* note 103, at 602.

107. *Id.*

108. FERRERA, ET AL., *supra* note 11, at 419.

individual or group uses the Internet, e-mail, or other electronic communication to stalk or harass another."[109] Harassment need not be limited to direct harassment by the stalker. In some instances, cyberstalkers obtain personal information about their victim from online and other sources, and then display that information on a website or online newsgroup or bulletin board, encouraging third-party strangers to harass the victim.[110]

One main difference of cyberstalking from real-world stalking, however, is the greater anonymity of the cyberstalker. "This uncertainty can cause a greater sense of panic among victims who are left to wonder if the cyberstalker is in another state, down the block, or in the next cubicle at work."[111] Minimal effort is needed by the cyberstalker to remain anonymous over the Internet, and yet, they may terrorize their victim greatly.[112]

There have been some cases of cyberstalking in the United States that are tragic. One such instance involved a man from Massachusetts who pleaded guilty to stalking and raping a 14-year old girl he met in a chat room.[113] In 1999, a graduate student of the University of San Diego was arrested after he terrorized five female university students by bombarding them with threatening and violent e-mails for one year. He sent e-mails such as "Reply to my e-mail or you will die" and "I'll give you until this Friday to answer my e-mail or I'll show up at your cell physiology class or go to your house." The cyberstalker pled guilty.[114]

Another case involved a 50-year old former security guard who terrorized his 28-year old victim "by impersonating her in various Internet chat rooms and online bulletin boards, where he posted, along with her telephone number and address, messages that she fantasized being raped."[115]

---

109. Valetk, *supra* note 102, at 15.

110. FERRERA, ET AL., *supra* note 11, at 420; CASEY, *supra* note 103, at 603.

111. Valetk, *supra* note 102, at 16.

112. *Id.*

113. *Id.* (citing Associated Press, *Lowell man pleads guilty to Internet stalking, raping 14-year-old girl*, BOSTON.COM, *available at* http://www.boston.com/news/daily/21/ internet_stalker.htm (last accessed Aug. 19, 2008)).

114. *Id.* (citing Joseph C. Mershman, *The Dark Side of the Web: Cyberstalking and the Need for Contemporary Legislation*, 24 HARV. WOMEN'S L.J. 255 (2001)); Attorney General of the United States, 1999 Report on Cyberstalking: A New Challenge for Law Enforcement and Industry, *available at* http://www.usdoj.gov/criminal/cybercrime/cyberstalking.htm (last accessed Aug. 19, 2008) [hereinafter U.S. Attorney General, 1999 Report].

115. U.S. Attorney General, 1999 Report, *supra* note 114.

This resulted in the victim — who rejected the romantic advances of the security guard — receiving knocks on her door from men saying they wanted to rape her. The cyberstalker likewise pled guilty.[116]

*b. Elements of Cyberstalking*

Based on the above discussion, the following elements of cyberstalking may be inferred:

(a) A pattern of conduct such as but not limited to the sending of an online message, or online impersonation of a person, or posting of personal information of another person online for public viewing, or any use of an electronic communication device

(b) with the intent of terrorizing, harassing, threatening, or otherwise causing fear to another, or placing another under surveillance, or any combination thereof

(c) without lawful justification.

## III. RELEVANT PHILIPPINE LAWS AND THEIR SUFFICIENCY

### *A. An Overview of Philippine Laws*

The main legislation concerning cybercrime in the Philippines is the e-Commerce Act of 2000. Although this law has been in consideration with the legislative body for some time, it was enacted only after the love bug virus was "accidentally unleashed" to the world. It is based on the United Nations Commission on International Trade Law (UNCITRAL) Model Law on e-Commerce.[117] An examination of the e-Commerce Act of 2000 will reveal that it mostly provides for the legal recognition of electronic documents and data messages, and how these are transmitted, under its second and third chapters, from Sections 6 to 24. It also has specific provisions on the carriage of goods using electronic commerce and electronic transactions in government, found under its third and fourth parts respectively. The final part begins at Section 30 and discusses the liability of a service provider, lawful access, and obligations of confidentiality. Section 33 finally provides for penalties for certain cybercrimes, such as hacking or cracking, viruses, and piracy.

116. *Id.*

117. 3 RECORD OF THE SENATE 405-06, S. 1902, 11th Cong., 2d Sess. (Feb. 16, 2000).

When the love bug virus struck the world and the perpetrator was traced to a Filipino residing in the Philippines, the closest law authorities could find to penalize the perpetrator was the Access Devices Regulation Act of 1998. This law essentially deals with access devices such as credit cards and their illegal use. It declares as unlawful a number of acts related to counterfeit access devices, unauthorized access devices, or access devices fraudulently applied for.

The primary penal legislation of the Philippines is the Revised Penal Code. This Code is rather old and takes its cue from the old Penal Code, which became effective on 14 July 1887 after it was directed to be applied in the Philippine islands by the Crown of Spain.[118] The old Penal Code was thereafter ordered revised by the Department of Justice, through Administrative Order No. 94, dated 18 October 1927, and, hence, the Revised Penal Code became effective on 1 January 1932.[119]

The only law to define stalking in the Philippines, the Anti-Violence Against Women and Their Children Act of 2004 is also be discussed in relation to cyberstalking and its potential applicability to the said crime. Also, since cyberstalking may involve harassment, it would not be distant to consider the Anti-Sexual Harassment Act of 1995.[120]

The succeeding Sections will now examine whether Philippine laws are sufficient to penalize the cybercrimes previously mentioned.

*B. Phishing*

As previously provided, the following are the elements of phishing:

> (a) That an offender solicits, requests, or otherwise induces another to provide personally identifying information
>
> (b) That such was done through the creation and sending of an electronic mail message, the creation of a website, or otherwise through the Internet
>
> (c) That such was made without right or authority to request or solicit such personally identifying information, or otherwise through false representation.[121]

118. REYES, BOOK ONE, *supra* note 6, at 21.

119. *Id.* at 20-21.

120. An Act Declaring Sexual Harassment Unlawful in the Employment, Education or Training Environment, and for other Purposes [Anti-Sexual Harassment Act of 1995], Republic Act No. 7877 (1995).

121. TALLY, *supra* note 85, at 3.

Section 33, the pertinent provision of the e-Commerce Act of 2000, provides as follows:

> 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.[122]

A perusal of this provision of the law will show that it is not applicable to phishing. An analysis of section 33 will show that hacking or cracking has the following elements:

> (a) the unauthorized access into or interference in a computer system/server or information and communication system; or
>
> (b) *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 communication system, including the introduction of computer viruses and the like
>
> (c) resulting in the corruption, destruction, alteration, theft, or loss of electronic data messages or electronic document.[123]

The said provision requires that there be an unauthorized access or interference; or any access in a computer or information and communication system without the knowledge and consent of the owner of the computer or information and communication system (computer). None of the elements of phishing involve unauthorized access or interference, or any access without the knowledge of the owner of the computer in order to corrupt, alter, steal, or destroy. As discussed in the previous chapter, phishers normally acquire personally identifying information by sending an e-mail providing a link to their sham website or by requesting the victim to e-mail them such information. Once the victim clicks on the link to the replica website, the phisher cannot be considered as accessing the computer of the victim. Rather, the victim accesses the fake website himself. Neither is there access on the part of the phisher when the victim e-mails his personally identifying information, for the victim sends the e-mail on his own volition using his own computer without interference on the part of the phisher.

122. e-Commerce Act of 2000, § 33 (a).

123. *Id.* (emphasis supplied).

Thus, when a victim follows the link to the phisher's website or sends his personally identifying information through e-mail, in no instance does the phisher gain access to or interferes with the victim's computer. Rather, it is the victim who, if at all, could be considered as accessing the website of the offender.

Neither can it be considered that the sending of e-mail by the phisher is the *unauthorized access, interference; or any access without consent* contemplated by the above provision. One must note that the *unauthorized access, interference; or any access without consent*[124] provided by said Section 33 is used to refer to hacking or cracking. The sending of an e-mail to another, particularly by a stranger, cannot be interpreted as unauthorized access or interference, or any access without consent. Such an interpretation would lead to the absurd result of any person sending an e-mail to another, even for legitimate reasons (e.g. such as to inquire about a certain matter, or to consult, or even to praise or commend another) would be liable for hacking or cracking. Under this interpretation, if, for instance, a person sends an e-mail to a professor, without the professor's consent, asking for advice on his or her thesis, that person may be held liable for hacking or cracking. Certainly, this was not the intent of the law. Whether or not that person even intended to hack, crack, or phish, this manner of interpreting Section 33 of the e-Commerce Act would make the sending of many e-mails a crime of hacking or cracking. An examination of the records of the Senate will show that the intent of the law is to penalize hacking or cracking, and not the mere sending of an e-mail.[125]

As can be gleaned, the elements of phishing are not square with the elements of Section 33, except maybe by a very far-stretch of one's imagination, which is not allowed in criminal law.[126]

The next Philippine law that may apply to phishing is the Access Devices Regulation Act of 1998. The pertinent provision of this law is section 9, which penalizes fraudulent acts in relation to access devices.[127] An access device is defined as

---

124. The full text of which provides "unauthorized access into or interference in a computer system/server or information and communication system; or any access … without the knowledge and consent of the owner of the computer or information and communications system …." *Id.*

125. *See generally* 3 RECORD OF THE SENATE 405-06, S. 1902, 11th Cong., 2d Sess. (Jan. 17, 2000 – Mar. 28, 2000).

126. *See* Laurel v. Abrogar, 483 SCRA 243 (2006).

127. Access Devices Regulation Act of 1998, § 9.

Sec. 9. Prohibited Acts. — The following acts shall constitute access device fraud and are hereby declared to be unlawful:

(a) producing, using, trafficking in one or more counterfeit access devices;

(b) trafficking in one or more unauthorized access devices or access devices fraudulently applied for;

(c) using, with intent to defraud, an unauthorized access device;

(d) using an access device fraudulently applied for;

(e) possessing one or more counterfeit access devices or access devices fraudulently applied for;

(f) producing, trafficking in, having control or custody of, or possessing device-making or altering equipment without being in the business or employment, which lawfully deals with the manufacture, issuance, or distribution of such equipment;

(g) inducing, enticing, permitting or in any manner allowing another, for consideration or otherwise to produce, use, traffic in counterfeit access devices, unauthorized access devices or access devices fraudulently applied for;

(h) multiple imprinting on more than one transaction record, sales slip or similar document, thereby making it appear that the device holder has entered into a transaction other than those which said device holder had lawfully contracted for, or submitting, without being an affiliated merchant, an order to collect from the issuer of the access device, such extra sales slip through an affiliated merchant who connives therewith, or, under false pretenses of being an affiliated merchant, present for collection such sales slips, and similar documents;

(i) disclosing any information imprinted on the access device, such as, but not limited to, the account number or name or address of the device holder, without the latter's authority or permission;

(j) obtaining money or anything of value through the use of an access device, with intent to defraud or with intent to gain and fleeing thereafter;

(k) having in one's possession, without authority from the owner of the access device or the access device company, an access device, or any material, such as slips, carbon paper, or any other medium, on which the access device is written, printed, embossed, or otherwise indicated;

(l) writing or causing to be written on sales slips, approval numbers from the issuer of the access device of the fact of

> 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).[128]

As phishing many times are intended to gather information about financial records and accounts of the intended victim, many kinds of information gathered by phishing may fall under this definition, such as account numbers, personal identification numbers, or other means of account access that can be used to obtain money, goods, services, or other things of value or to initiate a transfer of funds. It must be noted, however, that not all forms of phishing are aimed at gathering "access device" information or that information "that can be used to obtain money, goods, services, or any thing of value." Some forms of phishing are aimed at gathering personally identifying information that does not necessarily provide access. Phishing may, for example, be used to gather basic information such as names, date of birth, etc. that may be used to open a new account at a bank or even to apply for a loan. These may not be considered as account access, but rather as account creation. These may also be used to gain an alias to commit crimes so that the actual criminal cannot be traced. The theft of one's identity can have various purposes other than as a means of account access to obtain money, goods, services, or any other thing of value. Admittedly however, phishing may still be employed to

---

approval, where in fact no such approval was given, or where, if given, what is written is deliberately different from the approval actually given;

(m) making any alteration, without the access device holder's authority, of any amount or other information written on the sales slip;

(n) effecting transaction, with one or more access devices issued to another person or persons, to receive payment or any other thing of value;

(o) without the authorization of the issuer of the access device, soliciting a person for the purpose of:

(1) offering an access device; or

(2) selling information regarding or an application to obtain an access device; or

(p) without the authorization of the credit card system member or its agent, causing or arranging for another person to present to the member or its agent, for payment, one or more evidence or records of transactions made by credit card.

128. *Id.* § 3 (a) (emphasis supplied).

gather financial and account access information. Even so, as subsequently discussed, the Access Devices Regulation Act of 1998 may be difficult to apply.

The pertinent portions of section 9 of the Access Devices Regulation Act of 1998 are paragraphs (b), (c), (g), (i), (j), (k), and (n). Paragraphs (a), (d), and (e) are only concerned with counterfeit access devices or access devices fraudulently applied for, whereas phishing is more concerned with unauthorized access devices. A Counterfeit access device is defined as "any access device that is counterfeit, fictitious, altered, or forged, or an identifiable component of an access device or counterfeit access device;"[129] while access devices fraudulently applied for are defined as "any access device that was applied for or issued on account of the use of falsified document, falsified information, fictitious identities and address, or any form of false pretense or misrepresentation."[130] Phishing involves the theft of authentic personally identifying information, rather than the creation of fake information (i.e. counterfeit or fraudulently applied for).[131] Paragraph (f) deals with access device making or altering machines, such as credit card making machines. Paragraph (h), on the other hand, is concerned with multiple imprinting of transactions, sales slips, or other records. Thus, this involves a situation, for example, wherein a buyer purchases an item using a credit card and the seller or his agent makes two sales slips or enters the transaction twice for one purchase-item. Paragraphs (l) and (m) relate to sales slips, while paragraph (o) refers to unauthorized solicitation of access device applications. Paragraph (o) involves a situation wherein, for example, one solicits the credit card application of another, without authority from the credit card company. Paragraph (p) refers to credit cards and records of transactions. All these do not relate to phishing as they are concerned more with access device transactions or applications, or counterfeit access devices, or access devices as used in the physical world. They therefore do not involve the elements of phishing, which pertains to online identity theft.

Paragraphs (b), (c), (i), (j), (k), and (n) are concerned with the use or possession of unauthorized access devices[132] subsequent to their acquisition.

---

129. *Id.* § 3 (b).

130. *Id.* § 3 (c).

131. It should be noted that the definition of access device fraudulently applied for uses false pretense or misrepresentation in the application for or issuance of the access device, and not in obtaining or stealing of the access device.

132. Defined in Section 3, paragraph (c) as "any access device that is stolen, lost, expired, revoked, cancelled, suspended, or obtained with intent to defraud." Access Devices Regulation Act of 1998, § 3 (c).

It must be emphasized at this juncture that *phishing* is concerned with the theft of personally identifying information, rather than the subsequent use of it, as provided for by its elements. Moreover, one of the elements of phishing requires false representation in acquiring personally identifying information, which is not found in these paragraphs. Paragraph (b) penalizes the "trafficking in one or more unauthorized access devices or access devices fraudulently applied for."[133] Trafficking "means transferring, or otherwise disposing of, to another, or obtaining control of, with intent to transfer or dispose of."[134] Paragraph (c) penalizes "using, with intent to defraud, an unauthorized access device"[135] and paragraph (j) penalizes "obtaining money or anything of value through the use of an access device, with intent to defraud, or with intent to gain."[136] Again, not all forms of identity theft are aimed at obtaining money or anything of value, as previously mentioned. Paragraph (i) is concerned with the "disclosing of any information imprinted on the access device, such as, but not limited to, the account number or name or address of the device holder, without the latter's authority or permission."[137] This paragraph is also concerned with the subsequent use of access devices. Further, this paragraph requires for information to be imprinted on an access device, which is many times not the case in identity theft and phishing. The phisher may obtain information that is not necessarily imprinted on an access device. It is worth noting that the Access Devices Regulation Act of 1998 is mainly focused on credit cards and credit card fraud, referred to in the law as "access devices in commercial transactions."[138]

Paragraph (g) penalizes the "inducing, enticing, permitting or in any manner allowing another, for consideration or otherwise to produce, use, traffic in counterfeit access devices, unauthorized access devices or access devices fraudulently applied for."[139] To apply this paragraph to phishing would be stretching the law. Even if there is inducement, as provided for by paragraph (g), it is necessary that this leads to the production, use, or trafficking of unauthorized access devices. *Produce* is defined in the law as to design, alter, authenticate, duplicate or assemble.[140] A phishing attempt does

133. *Id.* § 9 (b).

134. *Id.* § 3 (l).

135. *Id.* § 9 (c).

136. *Id.* § 9 (j).

137. *Id.* § 9 (i).

138. Access Devices Regulation Act of 1998, § 2.

139. *Id.* § 9 (g).

140. *Id.* § 3 (k).

not 'produce' an unauthorized access device, but, rather, steals personally identifying information. It can be argued that once personally identifying information is stolen, some of them may thereafter be called *unauthorized* access devices. It must be mentioned again, however, that not all forms of personally identifying information can be considered as access devices (e.g. birthdays, blood type, and marital status). Neither does phishing involve the inducement or enticement of the victim to use or traffic in counterfeit or unauthorized access devices.

Indeed, the access devices regulation act would be difficult to apply, as it is not all encompassing and neither does it clearly penalize phishing. Emphasis must be placed on the fact that the Access Devices Regulation Act of 1998 was passed to combat credit-card fraud. As held by jurisprudence, "*penal statutes may not be enlarged* by implication or intent beyond the fair meaning of the language used; and may not be held to include offenses other than those which are *clearly* described, notwithstanding that the Court may think that Congress should have made them more comprehensive."[141]

Absent the applicability of these special penal laws, resort must then be made to the Revised Penal Code, the primary penal legislation of the Philippines. As phishing involves the deceptive inducement by the offender of the victim to provide him or her with personally identifying information, Chapter Six of Title 10 of the Revised Penal Code, or the chapter on deceits must necessarily be examined. Article 315 provides for the crime of swindling or estafa.[142] Although this article penalizes fraud by means of

141. Laurel v. Abrogar, 483 SCRA 243, 267 (2006) (emphasis supplied).

142. REVISED PENAL CODE, art. 315.

> Art. 315. Swindling (estafa). — Any person who shall defraud another by any of the means mentioned hereinbelow shall be punished by:
>
> 1st. The penalty of *prision correccional* in its maximum period to prision mayor in its minimum period, if the amount of the fraud is over 12,000 pesos but does not exceed 22,000 pesos, and if such amount exceeds the latter sum, the penalty provided in this paragraph shall be imposed in its maximum period, adding one year for each additional 10,000 pesos; but the total penalty which may be imposed shall not exceed twenty years. In such cases, and in connection with the accessory penalties which may be imposed under the provisions of this Code, the penalty shall be termed *prision mayor* or *reclusion temporal*, as the case may be.
>
> 2nd. The penalty of *prision correccional* in its minimum and medium periods, if the amount of the fraud is over 6,000 pesos but does not exceed 12,000 pesos;

3rd. The penalty of *arresto mayor* in its maximum period to *prision correccional* in its minimum period if such amount is over 200 pesos but does not exceed 6,000 pesos; and

4th. By *arresto mayor* in its maximum period, if such amount does not exceed 200 pesos, provided that in the four cases mentioned, the fraud be committed by any of the following means:

(1) With unfaithfulness or abuse of confidence, namely:

(a) By altering the substance, quantity, or quality or anything of value which the offender shall deliver by virtue of an obligation to do so, even though such obligation be based on an immoral or illegal consideration.

(b) By misappropriating or converting, to the prejudice of another, money, goods, or any other personal property received by the offender in trust or on commission, or for administration, or under any other obligation involving the duty to make delivery of or to return the same, even though such obligation be totally or partially guaranteed by a bond; or by denying having received such money, goods, or other property.

(c) By taking undue advantage of the signature of the offended party in blank, and by writing any document above such signature in blank, to the prejudice of the offended party or of any third person.

(2) By means of any of the following false pretenses or fraudulent acts executed prior to or simultaneously with the commission of the fraud:

(a) By using fictitious name, or falsely pretending to possess power, influence, qualifications, property, credit, agency, business or imaginary transactions, or by means of other similar deceits.

(b) By altering the quality, fineness or weight of anything pertaining to his art or business.

(c) By pretending to have bribed any Government employee, without prejudice to the action for calumny which the offended party may deem proper to bring against the offender. In this case, the offender shall be punished by the maximum period of the penalty.

(d) [By post-dating a check, or issuing a check in payment of an obligation when the offender therein were not sufficient to cover the amount of the check. The failure of the drawer of the check to deposit the amount necessary to cover his check within three (3) days from receipt of notice from the bank and/or the payee or holder that said check has been

deceit,[143] another one of its elements requires that there be "damage or prejudice capable of pecuniary estimation caused to the offended party or third person."[144] It has already been highlighted that phishing may not necessarily involve damage or prejudice to another that is capable of pecuniary estimation. What is involved in phishing is the theft of personally identifying information — the monetary value of which cannot be estimated. The pecuniary value of information of one's name, birthday, marital status, driver's license number, or social security number cannot be estimated, as certainly, these are not commodities or the kind of property that has an objective value. "It is necessary that the damage or prejudice be capable of pecuniary estimation, because the amount of the damage or prejudice is the basis of the penalty of estafa."[145] "The penalty in estafa is always a fine, hence, in estafa there is always money value. In the absence of such money value constituting damage to the offender, there is no estafa, except in estafa through forecasting, etc. The exact money value should be

---

dishonored for lack of insufficiency of funds shall be prima facie evidence of deceit constituting false pretense or fraudulent act. (As amended by R.A. 4885, approved June 17, 1967.)]

(e) By obtaining any food, refreshment or accommodation at a hotel, inn, restaurant, boarding house, lodging house, or apartment house and the like without paying therefor, with intent to defraud the proprietor or manager thereof, or by obtaining credit at hotel, inn, restaurant, boarding house, lodging house, or apartment house by the use of any false pretense, or by abandoning or surreptitiously removing any part of his baggage from a hotel, inn, restaurant, boarding house, lodging house or apartment house after obtaining credit, food, refreshment or accommodation therein without paying for his food, refreshment or accommodation.

(3) Through any of the following fraudulent means:

(a) By inducing another, by means of deceit, to sign any document.

(b) By resorting to some fraudulent practice to insure success in a gambling game.

(c) By removing, concealing or destroying, in whole or in part, any court record, office files, document or any other papers.

143. LUIS B. REYES, THE REVISED PENAL CODE: CRIMINAL LAW BOOK TWO 732 (15th ed. 2001) [hereinafter REYES, BOOK TWO].

144. Garcia v. People, 410 SCRA 582, 587 (2003); People v. Saulo, 344 SCRA 605, 615-616 (2000). *See also* REYES, BOOK TWO, *supra* note 143, at 732.

145. REYES, BOOK TWO, *supra* note 143, at 733.

shown."[146] While it is not disputed that phishing involves deceit or false pretenses, particularly as provided for under Article 315, subsection 2 (a),[147] an essential element of estafa by false pretenses is that the offended party be deprived of his property. "The offender must be able to obtain something from the offended party because of the false pretense, without which the offended party would not have parted with it."[148] In fine, estafa requires, as one of its elements, that damage capable of pecuniary estimation be caused to the victim or complainant. This contemplates objects the monetary value of which can be determined — which is not the case in phishing as personally identifying information is intangible property — its value not susceptible to objective valuation.

This same argument may be set forth in considering Article 318 of the Revised Penal Code, the pertinent portion of which provides:

> Art. 318. *Other deceits*. – The penalty of *arresto mayor and a fine of not less than the amount of the damage caused and not more than twice such amount* shall be imposed upon any person who shall defraud or damage another by any other deceit not mentioned in the preceding articles of this chapter.

Again, this provision of law requires that damage be made to the offended party, as this becomes the basis of the fine to be imposed on the offender.[149] In like manner with estafa, not all forms of phishing are covered by Article 318, for personally identifying information is not capable of pecuniary estimation. Again, as held by the Supreme Court, penal statutes cannot be expanded beyond what was contemplated by Congress in drafting the law.[150]

---

146. LEONOR D. BOADO, NOTES AND CASES ON THE REVISED PENAL CODE 772 (2004 ed.) (emphasis supplied).

151. REYES, BOOK TWO, *supra* note 143, at 767 (citing People v. Gines, et al., 61 O.G. 1365 (Court of Appeals 6)). Luis B. Reyes notes that false pretense, fraudulent acts or means are indispensable to estafa under Article 315, subsection 2 (a) of the Revised Penal Code. He states:

> In the prosecution of estafa under Article 315, paragraph 2 (a) of the Revised Penal Code, it is indispensable that the element of deceit, consisting of false statement or fraudulent representation of the accused, be made prior to, or, at least simultaneously with, the delivery of the thing by the complainant, it being essential that such false statement or fraudulent representation constitutes the very cause or the only motive which induces the complainant to part with the thing.

148. *Id.* at 772.

149. *Id.* at 815.

150. Laurel v. Abrogar, 483 SCRA 243, 267 & 273 (2006).

Phishing is concerned with the theft of identity, and not its subsequent use. It is much like theft of personal property, which merely requires the taking of personal property belonging to another without the consent of the owner, with the intent to gain.[151] It is not concerned with how the stolen property is subsequently used. This begs the question of whether theft under the Revised Penal Code is applicable to phishing. The relevant article of the Revised Penal Code is Article 308, which provides, thus:

> Art. 308. Who are liable for theft. — Theft is committed by any person who, with intent to gain but without violence against or intimidation of persons nor force upon things, shall take personal property of another without the latter's consent.[152]

The case of *Laurel v. Abrogar*[153] is enlightening as to the applicability of this provision of law. Although the case was brought by the Philippine Long Distance Telephone Company against the petitioner for the "theft" of international telephone calls, the Court's pronouncements may apply to identity theft and phishing. It provides as follows:

> One is apt to conclude that "personal property" *standing alone*, covers both tangible and intangible properties and are subject of theft under the Revised Penal Code. But the words "Personal property" under the Revised Penal Code must be considered in tandem with the word "take" in the law. The statutory definition of "taking" and movable property indicates that, clearly, not all personal properties may be the proper subjects of theft. The general rule is that, only movable properties *which have physical or material existence* and susceptible of occupation by another are proper subjects of theft.[154]

Personally identifying information, which have no *physical or material existence*, are not the proper subject of theft as penalized by the Revised Penal Code.

The same case could also shed some light as to the applicability of the e-Commerce Act of 2000, the Access Devices Regulation Act of 1998, and the Revised Penal Code as penal laws. The Court held in the case that penal laws are to be construed strictly.[155] It provides, thus:

> Penal statutes may not be enlarged by implication or intent beyond the fair meaning of the language used; and may not be held to include offenses

151. REVISED PENAL CODE, art. 308.

152. *Id.*

153. *Laurel*, 483 SCRA at 243.

154. *Id.* at 268-69 (emphasis supplied).

155. *Id.* at 266.

> other than those which are clearly described, notwithstanding that the Court may think that Congress should have made them more comprehensive ….
>
> As Chief Justice John Marshall declared, "it would be dangerous, indeed, to carry the principle that a case which is within the reason or mischief of a statute is within its provision, so far as to punish a crime not enumerated in the statute because it is of equal atrocity, or of kindred character with those which are not enumerated."[156] When interpreting a criminal statute that does not explicitly reach the conduct in question, the Court should not base an expansive reading on inferences from subjective and variable understanding.[157]

*C. Denial of Service*

The following are the elements of a denial of service attack:

(a) The intentional unauthorized access, interference, or disruption of a computer or an electronic communication device or online service; or

(b) the intentional unauthorized consumption of computer network resources; or

(c) the intentional unauthorized alteration of the configuration information of a computer or electronic communication device

(d) in order to hinder or prevent legitimate access to or of a computer or network or online service.

Again, these elements will be examined in light of Section 33 of the e-Commerce Act:

> 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* ….[158]

As already mentioned in the previous Section, an analysis of section 33 will show that hacking or cracking has the following elements:

---

156. Id. at 267 (citing United States v. Wiltberger, 18 U.S. 76 (1820)).

157. *Id.* (citing Dowling v. United States, 473 U.S. 207 (1985)).

158. e-Commerce Act of 2000, § 33 (a) (emphasis supplied).

> (a) the unauthorized access into or interference in a computer system/server or information and communication system; or
>
> (b) 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 communication system, including the introduction of computer viruses and the like
>
> (c) resulting in the corruption, destruction, alteration, theft, or loss of electronic data messages or electronic document.[159]

A cursory examination of the above provision might lead to the interpretation that hacking or cracking can be committed either by the unauthorized access into or interference in a computer system or server or information and communication system alone (i.e. without the necessity of a resultant corruption, destruction, alteration, theft, or loss of electronic data messages or electronic documents); or by 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 communication 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. Thus, in this interpretation, while the unauthorized access or interference does not require a resultant corruption, destruction, alteration, theft, or loss of electronic data messages or electronic documents, the second part, referring to *any access in order to corrupt, alter, steal, or destroy*, requires for there to be corruption, destruction, alteration, theft, or loss of electronic data messages or documents. Indeed, if this interpretation were to be taken, denial of service attacks would be punishable under the electronic commerce act of 2000 as constituting *interference in a computer system/server or information and communication system* under the first part of Section 33. Nevertheless, a deeper examination of this law reveals that such an interpretation is erroneous and overly broad.

It is overly broad since — as unauthorized access or interference is not qualified by the need for a resultant corruption, destruction, alteration, theft or loss — any form of unauthorized access or interference would be considered as hacking or cracking, punishable under the e-Commerce Act, whether or not there was any intent on the part of the actor or doer to corrupt, destroy, alter, or steal. Accidental interference or interference without the knowledge on the part of the actor or doer or the owner of the computer would be punishable under this interpretation. An absurd result

159. *Id.*

would emerge wherein people, unknowledgeable or perhaps unfamiliar with technology, could be penalized as a hacker or cracker, perhaps by accidentally triggering software that executes denial of service attacks. Given this absurdity, the e-Commerce Act of 2000 may be difficult to apply, given the legal principle that penal statutes must be construed liberally in favor of the accused and strictly against the state.[160]

More importantly, such an interpretation is erroneous as an examination of legislative intent will show that the *resulting corruption, destruction, alteration, theft, or loss* is meant to qualify unauthorized access and interference. The original definition of hacking or cracking did not even include the clause "any access in order to corrupt, alter, steal, or destroy." Rather, it provided:

> "Hacking" or "Cracking" refers to unauthorized access into or interference in a computer system/server by or through the use of a computer or a computer system or other means in the computer or in another computer without the knowledge or consent of the owner of the computer or system, including the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of data messages.[161]

This definition of hacking or cracking shows that *unauthorized access or interference* was not meant to constitute a crime on its own, but requires that corruption, destruction, alteration, theft, or loss of data messages accompany it. Senator Aquilino Pimentel, Jr., the author of the above definition of hacking or cracking,[162] even clarified during the Senate deliberations that

> the definition here does not end in just stating that there is interference or unauthorized access. It goes on to say "resulting in the corruption, destruction, alteration, theft or loss of data messages." That last part should make a lot of difference between innocent hacking or cracking or whatever the term would be, because what makes this a crime is not only the unauthorized access of interference but also the resultant destruction, alteration, theft or loss of the data messages.[163]

An examination of the legislative intent of this penal provision will show that it was meant to penalize hacking or cracking per se, including the introduction of viruses, but not denial of service attacks, as subsequently shown.

---

160. Campomanes v. People, 511 SCRA 285, 300 (2006).

161. 3 RECORD OF THE SENATE 731, S. 1902, 11th Cong., 2d Sess. (Mar. 21, 2000).

162. *Id.*

163. *Id.* at 732.

Indeed, denial of service attacks may constitute unauthorized access or interference falling under the first element of section 33, as denial of service attacks involve either the intentional unauthorized access, interference, or disruption of a computer or an electronic communication device; the intentional unauthorized consumption of computer network resources; or the intentional unauthorized alteration of the configuration information of a computer or electronic communication device. These acts are clearly a form of unauthorized access or interference which is one of the elements of the above cited Section 33. The difference, however, lies in the result, for while Section 33 requires that there be *corruption, destruction, alteration, theft, or loss of electronic data messages or electronic documents*, denial of service attacks result in the *hindrance or prevention of legitimate access to or of a computer or network or online service*. It must be noted that an electronic data message refers to information generated, sent, received, or stored by electronic, optical, or similar means.[164] As provided in the discussion in the previous section, in most denial of service attacks, no electronic data message as defined by the e-Commerce Act of 2000 is corrupted, destroyed, altered, or stolen. At best, electronic data messages are prevented from reaching their destinations or prevented from being retrieved, more often by overloading a system. The target of denial of service attacks are access to or of a computer or network or online service, rather than the electronic data messages themselves.

While it may be argued that denial of service attacks may constitute an alteration or loss of electronic data messages, a conviction under this interpretation would be difficult. The hindrance to or prevention of access does not necessarily result into the alteration or loss of an electronic data message. It may be that the electronic data message, such as a website or an e-mail, remains at a server and access to it is hindered. In this scenario, the electronic data message is neither altered nor loss.

The law is not clear as to whether the e-Commerce Act of 2000 indeed covers denial of service attacks. Moreover, it is apparent during the Senate deliberations that the law was meant to penalize hacking or cracking per se, and not denial of service attacks. The Senate deliberations reveal that the law was meant to deal with unauthorized access or interference or any access that results in the corruption, destruction, alteration, theft, or loss of electronic data messages or electronic documents, and not the form of access or interference that prevents or hinders access to a computer, network, or online service. "It is a well-known rule of legal hermeneutics that penal or

164. e-Commerce Act of 2000, § 5 (c).

criminal laws are strictly construed against the state and liberally in favor of the accused."[165] The Supreme Court has ruled:

> If the language of the law were ambiguous, the court will lean more strongly in favor of the defendant than it would if the statute were remedial, as a means of effecting substantial justice. The law is tender in favor of the rights of an individual. It is the philosophy of caution before the State may deprive a person of life or liberty that animates one of the most fundamental principles in our Bill of Rights, that every person is presumed innocent until proven guilty.[166]

Given the inapplicability of the e-Commerce Act of 2000, or the difficulty of finding a conviction under this law, the Revised Penal Code must then be examined.

A chapter of the Revised Penal Code that could possibly apply to denial of service attacks is the chapter on malicious mischief under Title 10. Nevertheless, an examination of the provisions on malicious mischief will yield the conclusion that a prosecution of denial of service attacks under this chapter will fail. The relevant provision is Article 327, which provides that "any person who shall deliberately cause to the property of another any damage not falling within the terms of the next preceding chapter, shall be guilty of malicious mischief."[167]

Scrutinizing this provision and the jurisprudence interpreting it will show that its elements are:

> (a) That the offender deliberately caused damage to the property of another;
>
> (b) That such act does not constitute arson or other crimes involving destruction;
>
> (c) That the act of damaging another's property be committed merely for the sake of damaging it.[168]

Similar to the e-Commerce Act of 2000, it would be difficult to apply this provision of law, if at all, to denial of service attacks. In no instance do the elements of denial of service attacks include damage or destruction as required by Article 327. Damage deliberately caused to the property of

165. People v. Bon, 506 SCRA 168, 207 (2006) (citing Valencia v. Court of Appeals, 401 SCRA 666, 680 (2003)).

166. *Id.* at 207-08.

167. REVISED PENAL CODE, art. 327.

168. Valeroso v. People, 412 SCRA 257, 261 (2003). *See also* REYES, BOOK TWO, *supra* note 143, at 837.

another is an essential element of malicious mischief.[169] Further, "damage means not only loss but also diminution of what is a man's own. Thus, damage to another's house includes defacing it."[170] Denial of service attacks does not involve destruction of property. Rather, they involve unauthorized access, interference, disruption, consumption of computer network resources, or the alteration of configuration information of a computer or electronic communication device in order to prevent or hinder legitimate access to a computer, network, or online service. Preventing or hindering legitimate access to a computer, network, or online service is not destruction but obstruction.

Even if it is argued that the consumption of network resources or the alteration of configuration information could be a form of destruction of property, such argument would be a far stretch and would fail. Network resources or configuration information could not have been the kind of property contemplated by legislators when formulating the Revised Penal Code. Moreover, the consumption or alteration of these resources or configuration information could not be a form of destruction as contemplated by Article 327. Again, the principles laid down in the case of *Laurel v. Abrogar* apply in interpreting Article 327, being part of the Revised Penal Code. Although this case involved the supposed theft of international telephone calls, it is enlightening in interpreting the Revised Penal Code and other penal laws. In holding that international telephone calls could not have been the personal property contemplated by the Revised Penal Code, the Supreme Court said,

> In defining theft, under Article 308 of the Revised Penal Code, as the taking of personal property without the consent of the owner thereof, the Philippine legislature could not have contemplated the human voice which is converted into electronic impulses or electrical current which are transmitted to the party called through the PSTN of respondent PLDT and the ISR of Baynet Card Ltd. within its coverage. When the Revised Penal Code was approved, on December 8, 1930, international telephone calls and the transmission and routing of electronic voice signals or impulses emanating from said calls, through the PSTN, IPL and ISR, were still non-existent. *Case law is that, where a legislative history fails to evidence congressional awareness of the scope of the statute claimed by the respondents, a narrow interpretation of the law is more consistent with the usual approach to the*

169. Caballes v. Department of Agrarian Reform, 168 SCRA 247, 257 (1988).

170. REYES, BOOK TWO, *supra* note 143, at 839 (citing People v. Asido, et al., 59 O.G. 3646 (Court of Appeals)).

> *construction of the statute. Penal responsibility cannot be extended beyond the fair scope of the statutory mandate.*[171]

As can be gathered from this pronouncement, there must be congressional awareness of the activity being claimed as falling within the scope of a penal statute at the time of its enactment for that activity to be considered as indeed within its scope. Otherwise, a narrow interpretation of the law must be adopted, as penal statutes cannot be expanded by implication. Consumption of network resources and alteration of configuration information as constituting damage to property could not have been contemplated by legislators when the Revised Penal Code was enacted, given the fact that computer networking was non-existent when the Revised Penal Code was approved on 8 December 1930.[172]

Articles 328[173] and 329[174] provide for the penalties imposed for violations of Article 327. Special consideration must be made to Article 330,

---

171. Laurel v. Abrogar, 483 SCRA 243, 273 (2006) (emphasis supplied).

172. *See generally* Kristula, *supra* note 34; FERRERA, ET AL., *supra* note 11; Mary Bellis, The History of Computers, *available at* http://inventors.about.com/library/blcoindex.htm (last accessed Aug. 19, 2008).

173. REVISED PENAL CODE, art. 328.

> Art. 328. *Special cases of malicious mischief.* — Any person who shall cause damage to obstruct the performance of public functions, or using any poisonous or corrosive substance; or spreading any infection, or contagion among cattle; or who cause damage to the property of the National Museum or National Library, or to any archive or registry, waterworks, road, promenade, or any other thing used in common by the public, shall be punished:
>
> By *prision correccional* in its minimum and medium periods, if the value of the damage caused exceeds 1,000 pesos;
>
> By *arresto mayor*, if such value does not exceed the abovementioned amount but it is over 200 pesos; and
>
> By *arresto menor*, if such value does not exceed 200 pesos.

174. *Id.* art. 329.

> Art. 329. Other mischiefs. – The mischiefs not included in the next preceding article shall be punished:
>
> By *arresto mayor* in its medium and maximum periods, if the value of the damage caused exceeds 1,000 pesos;
>
> By *arresto mayor* in its minimum and medium periods, if such value is over 200 pesos but does not exceed 1,000 pesos; and

as it concerns damage and obstruction to means of communication. It provides:

> Art. 330. *Damage and obstruction to means of communication.* – The penalty of *prision correccional* in its medium and maximum periods shall be imposed upon any person who shall damage any railway, telegraph or telephone lines.
>
> If the damage shall result in any derailment of cars, collision or other accident, the penalty of *prision mayor* shall be imposed, without prejudice to the criminal liability of the offender for the other consequences of his criminal act.
>
> For the purposes of the provisions of this article, the electric wires, traction cables, signal system and other things pertaining to railways, shall be deemed to constitute an integral part of a railway system.[175]

This provision explicitly mentions telegraph or telephone lines. Denial of service attacks clearly do not fall under this article as they do not involve the damage of telegraph or telephone lines. The obstruction involved in denial of service attacks are not obstruction of the physical network, but rather of the logical or electronic network (i.e. the system of communication between computers through the physical network).

*D. Cyberstalking*

Cyberstalking has the following elements:

> (a) A pattern of conduct such as but not limited to the sending of an online message, or online impersonation of a person, or posting of personal information of another person online for public viewing, or any use of an electronic communication device
>
> (b) with the intent of terrorizing, harassing, threatening, or otherwise causing fear to another, or placing another under surveillance, or any combination thereof
>
> (c) without lawful justification.

Again, these elements will be examined in light of the primary cybercrime legislation of the Philippines, the e-Commerce Act of 2000. An examination of Section 33[176] of this law will reveal that it is nowhere near covering the

---

> By *arresto menor* or fine of not less than the value of the damage caused and not more than 200 pesos, if the amount involved does not exceed 200 pesos or cannot be estimated.

175. *Id.* art. 330.

176. e-Commerce Act of 2000, § 33 (a).

elements of cyberstalking. Although cyberstalking requires that there be use of an electronic communication device, it does not require that such use be unauthorized or constitute interference or access without the knowledge and consent of the owner of the computer. In cyberstalking, the use of an electronic communication device may be authorized, such as using a chatroom or an online bulletin board. Secondly, the abovementioned provision penalizes intrusion that results into corruption, destruction, alteration, theft, or loss of electronic data messages or electronic documents. Cyberstalking, on the other hand, does not concern itself with electronic data messages or electronic documents per se. Rather, it is concerned with the use of electronic communication devices to terrorize, harass, threaten, cause fear, or place a victim under surveillance. While Section 33 above deals with the integrity of electronic data messages and electronic documents, cyberstalking is more concerned with the content of these messages, as well as how they are used. Further, cyberstalking is not necessarily limited to electronic data messages, such as when cyberstalkers impersonate their victim in a chatroom, and encourage others in that chatroom to somehow offend the victim.

The next law that could find applicability to cyberstalking is the Anti-Violence Against Women and Their Children Act of 2004. This law is the only law in the Philippines that defines stalking, which is as follows:

> Sec. 3. Definition of Terms. – As used in this Act,
>
> …
>
> (d) Stalking refers to an intentional act committed by a person who, knowingly and without lawful justification follows the woman or her child or places the woman or her child under surveillance directly or indirectly or a combination thereof.[177]

This definition must be placed in context with section 5 of the same law, which provides for what acts constitutes violence against women and their children, and are penalized under Section 6. The relevant portions of Section 5 are paragraphs (h) and (i). Paragraph (h) provides:

> Engaging in purposeful, knowing, or reckless conduct, personally or through another, that alarms or causes substantial emotional or psychological distress to the woman or her child. This shall include, but not be limited to, the following acts:
>
> (1) Stalking or following the woman or her child in public or private places;

177. Anti-Violence Against Women and Children Act of 2004, § 3 (d).

(2) Peering in the window or lingering outside the residence of the woman or her child;

(3) Entering or remaining in the dwelling or on the property of the woman or her child against her/his will;

(4) Destroying the property and personal belongings or inflicting harm to animals or pets of the woman or her child; and

(5) Engaging in any form of harassment or violence;[178]

While paragraph (i) provides, "Causing mental or emotional anguish, public ridicule or humiliation to the woman or her child, including, but not limited to, repeated verbal and emotional abuse, and denial of financial support or custody of minor children of access to the woman's child/children."

Paragraph (h) and (i) may be applicable to cyberstalking. Although paragraph (h) enumerates acts in subparagraphs (1) to (4) which are not performed online or do not involve computers, subparagraph (5) provides for a catch-all provision as engaging in any form of harassment or violence. It is unfortunate though that the law did not define harassment or violence. Hence, resort to the lexicon meaning of harassment and violence must be made.[179] The dictionary provides that to harass is to annoy persistently; or to disturb or torment persistently.[180] Violence on the other hand is defined as exertion of physical force so as to injure or abuse; or intense, turbulent, or furious and often destructive action or force.[181] Juxtaposed with the second element of cyberstalking, subparagraph (5) of paragraph (h) may encompass online and electronic forms of cyberstalking. Nevertheless, it may be argued that applying the statutory construction principle of *ejusdem generis*,[182] subparagraph (5) may be limited only to physical forms of harassment or violence, as the enumeration prior to subparagraph (5) is limited to physical forms. The principle of *ejusdem generis* provides that

> while general words or expressions in a statute are, as a rule, accorded their full, natural and generic sense, *they will not be given such meaning if they are used in association with specific words or phrases*. The general rule is that *where a general word or phrase follows an enumeration of particular and specific words of the*

178. e-Commerce Act of 2000, § 33.

179. AGPALO, *supra* note 7, at 180.

180. MERRIAM-WEBSTER DICTIONARY ONLINE, *available at* http://www.merriam-webster.com/dictionary/harass (last accessed Aug. 19, 2008).

181. MERRIAM-WEBSTER DICTIONARY ONLINE, *available at* http://www.merriam-webster.com/dictionary/violence (last accessed Aug. 19, 2008).

182. Guinhawa v. People, 468 SCRA 278, 299 (2005); Villamor Golf Club v. Pehid, 472 SCRA 36, 47 (2005).

> *same class or where the latter follow the former, the general word or phrase is to be construed to include, or be restricted to, persons things or cases akin to, resembling, or of the same kind or class as those specifically mentioned.*[183]

Paragraph (i) may also encompass cyberstalking as it, together with Section 6, penalizes acts with cause mental or emotional anguish to a woman or her child. It does not take much to imagine how online messages, online impersonation, and other forms of cyberstalking may cause mental anguish to others.

Although the Anti-Violence Against Women and Their Children Act may apply to cyberstalking, one thing lacking though with this law is that it requires the victim to be a woman or her child. It does not cover men, who, according to the study provided by the organization WHOA, comprise 22.5% of the victims of cyberstalking.[184] Despite the fact that 73.5% of victims are female, it must be pointed out that males may also be the victims of cyberstalking. Male bosses and managers, for example, may be the subject of attack of disgruntled employees turned cyberstalkers. The same may apply for male teachers and professors, as well as men with incensed ex-lovers. To this extent, the Anti-Violence Against Women and Their Children Act is insufficient.

This same insufficiency may be said to exist under the Anti-Sexual Harassment Act of 1995. The Anti-Sexual Harassment Act of 1995 was designed to prevent, or at least make unlawful, sexual harassment in the employment, education, and training environment.[185] For this law to apply, there is thus a necessity that there must be a work, education, or training environment, in which an employer, employee, manager, supervisor, agent of the employer, teacher, instructor, professor, coach, trainer, or any other person having authority, influence, or moral ascendancy over another demands, requests, or asks for sexual favors.[186] Further, such sexual favor

---

183. AGPALO, *supra* note 7, at 213 (emphasis supplied).

184. WHOA, *supra* note 101, at 213.

185. Anti-Sexual Harassment Act of 1995, § 2.

> Sec. 2. Declaration of Policy. - The State shall value the dignity of every individual, enhance the development of its human resources, guarantee full respect for human rights, and uphold the dignity of workers, employees, applicants for employment, students or those undergoing training, instruction or education. Towards this end, all forms of sexual harassment in the employment, education or training environment are hereby declared unlawful.

186. *Id.* § 3.

Sec. 3. Work, Education or Training-Related, Sexual Harassment Defined. - Work, education or training-related sexual harassment is committed by an employer, employee, manager, supervisor, agent of the employer, teacher, instructor, professor, coach, trainor, or any other person who, having authority, influence or moral ascendancy over another in a work or training or education environment, demands, requests or otherwise requires any sexual favor from the other, regardless of whether the demand, request or requirement for submission is accepted by the object of said Act.

(a) In a work-related or employment environment, sexual harassment is committed when:

(1) The sexual favor is made as a condition in the hiring or in the employment, re-employment or continued employment of said individual, or in granting said individual favorable compensation, terms of conditions, promotions, or privileges; or the refusal to grant the sexual favor results in limiting, segregating or classifying the employee which in any way would discriminate, deprive or diminish employment opportunities or otherwise adversely affect said employee;

(2) The above acts would impair the employee's rights or privileges under existing labor laws; or

(3) The above acts would result in an intimidating, hostile, or offensive environment for the employee.

(b) In an education or training environment, sexual harassment is committed:

(1) Against one who is under the care, custody or supervision of the offender;

(2) Against one whose education, training, apprenticeship or tutorship is entrusted to the offender;

(3) When the sexual favor is made a condition to the giving of a passing grade, or the granting of honors and scholarships, or the payment of a stipend, allowance or other benefits, privileges, or consideration; or

(4) When the sexual advances result in an intimidating, hostile or offensive environment for the student, trainee or apprentice.

Any person who directs or induces another to commit any act of sexual harassment as herein defined, or who cooperates in the

must be requested in return for some advantage or privilege, such as employment, or a more favorable compensation, or the granting of passing grades, or honors and scholarships.[187] Surely, the Anti-Sexual Harassment Act of 1995 may apply to cyberstalking if the offender were one in a position of authority, influence, or moral ascendancy in a work, education, or training environment. Unfortunately, as previously discussed, cyberstalking is not limited to these environments. The elements of cyberstalking do not require any form of relationship, clearly making the Anti-Sexual Harassment Act of 1995 insufficient on this point alone. A cyberstalker may be an infuriated former lover or a rejected suitor, for example, in which case this law would not find any application.

Moreover, the cyber offender need not be someone exercising authority, influence, or moral ascendancy. In fact, it is quite possible for the reverse to be true — the cyberstalker being the one under the authority of another. As aforementioned, a cyberstalker may be an employee, rather than an employer; or a student rather than a professor, in which case the Anti-Sexual Harassment Act of 1995 would definitely not apply.

The next law to be examined is the Revised Penal Code. The pertinent provisions of this code are Articles 282 and 283, which provide as follows:

> Art. 282. *Grave threats*. — Any person who shall threaten another with the infliction upon the person, honor or property of the latter or of his family of any wrong amounting to a crime, shall suffer:
>
> (1) The penalty next lower in degree than that prescribed by law for the crime he threatened to commit, if the offender shall have made the threat demanding money or imposing any other condition, even though not unlawful, and said offender shall have attained his purpose. If the offender shall not have attained his purpose, the penalty lower by two degrees shall be imposed.
>
> If the threat be made in writing or through a middleman, the penalty shall be imposed in its maximum period.
>
> (2) The penalty of *arresto mayor* and a fine not exceeding 500 pesos, if the threat shall not have been made subject to a condition.[188]

---

commission thereof by another without which it would not have been committed, shall also be held liable under this Act.

187. *Id.*; Aquino v. Acosta, 380 SCRA 1, 10-11 (2002).

188. REVISED PENAL CODE, art. 282.

> Art. 283. *Light threats*. — Any threat to commit a wrong not constituting a crime, made in the manner expressed in subdivision 1 of the next preceding article, shall be punished by *arresto mayor*.[189]

A perusal of the above provisions will show that acts punishable as grave threats are:

> (a) By threatening another with the infliction upon his person, honor, or property or that of his family of any wrong amounting to a crime, and demanding money or imposing any other condition, even though not unlawful, and the offender attained his purpose;
>
> (b) By making such threat without the offender attaining his purpose; or
>
> (c) By threatening another with the infliction upon his person, honor, or property or that of his family of any wrong amounting to a crime, the threat not being subject to a condition.[190]

The difference between these methods of committing grave threats is on whether or not a condition was imposed in making the threat, and if one was imposed, on whether such condition was attained. The common elements for the commission of grave threats are that:

> (a) The offender threatens another person with the infliction upon the latter's person, honor or property, or upon that of the latter's family, of any wrong; and
>
> (b) That such wrong amounts to a crime.[191]

Light threats, on the other hand, are committed when the following elements are present:

> (a) That the offender makes a threat to commit a wrong;
>
> (b) That the wrong does *not* constitute a crime; and
>
> (c) That there is a demand for money or that other condition is imposed even though not unlawful.[192]

The main difference between grave threats and light treats is that, in grave threats, the threat must amount to a crime.

---

189. *Id*. art. 283.

190. REYES, BOOK TWO, *supra* note 143, at 573.

191. *Id*. at 574.

192. *Id*. at 580.

Indeed, these crimes may encompass online threats such as when a threat to kill is made through e-mail or through some other electronic communication device. An e-mail, for example, that states "Reply to my e-mail or you will die" can be covered under these provisions, particularly under paragraph (1) of Article 282, as a threat to kill — killing being a crime under Chapter One of Title Eight[193] of the Revised Penal Code — is made, accompanied by a condition that the receiver must reply to the offender's e-mail. These two provisions of the Revised Penal Code, however, do not capture the entire essence of cyberstalking as they are limited to threats, but do not cover harassment, impersonation, or surveillance, such as when the cyberstalker impersonates a victim in a chat room and encourages others to harass her or posts personal information of another for online viewing. Cyberstalking contemplates a pattern of conduct involving more than just a single threat. It must be a series of actions using electronic communication devices that terrorizes the victim. While cyberstalking may include threats from the cyberstalker, other acts may be equally terrifying to a victim. The mere act of a cyberstalker of persistently sending love letters anonymously through e-mail (without threats), for example, may be terrifying.

Under the same section, Section Three of Chapter Two of Title Nine[194] of the Revised Penal Code, is the crime on coercions. Articles 286 and 287 provide as follows:

> Art. 286. *Grave coercions*. – The penalty of *prision correccional* and a fine not exceeding six thousand pesos shall be imposed upon any person who, without authority of law, shall, by means of violence, threats or intimidation, prevent another from doing something not prohibited by law, or compel him to do something against his will, whether it be right or wrong.
>
> If the coercion be committed in violation of the exercise of the right of suffrage, or for the purpose of compelling another to perform any religious act or to prevent him from exercising such right or from so doing such act, the penalty next higher in degree shall be imposed.[195]
>
> Art. 287. *Light coercions*. – Any person who, by means of violence, shall seize anything belonging to his debtor for the purpose of applying the same to the payment of the debt, shall suffer the penalty of *arresto mayor* in its

193. Title Eight is entitled Crimes against Persons, and Chapter One of this title deals with the destruction of life.

194. Title Nine deals with Crimes against Personal Liberty and Security. Chapter Two of this title is dedicated to Crimes Against Security, of which Section Three, entitled "Threats and coercion," is part.

195. REVISED PENAL CODE, art. 286.

> minimum period and a fine equivalent to the value of the thing, but in no case less than 75 pesos.
>
> Any other coercion or unjust vexation shall be punished by *arresto menor* or a fine ranging from 5 to 200 pesos, or both.[196]

Grave coercions involve either the prevention of another from doing something not prohibited by law through violence, threats or intimidation; or the compulsion of another to do something against his will, be it right or wrong, also through violence, threats, or intimidation.[197] It has been noted that the difference between threats and coercion is that in threats, the harm or wrong is future and conditional, whereas in coercion, the harm or wrong is immediate, personal, and direct.[198] Coercion involves force or violence that must be immediate, actual, or imminent.[199] Further, it has also been noted that while threats may be through an intermediary or in writing, coercion cannot be so.[200] This is consistent with the need for coercion to be immediate, actual, or imminent, for threats or intimidation made through an intermediary or in writing would not have the qualities of immediacy, actuality, and imminence.

The relevant portion of light coercions is the second paragraph, as the first paragraph requires a debtor-creditor relationship,[201] which is not essential in cyberstalking. The second paragraph makes reference to unjust vexation. Unjust vexation includes "any human conduct which, although not productive of some physical or material harm would, however, unjustly annoy or vex an innocent person."[202] "The paramount question to be considered, in determining whether the crime of unjust vexation is committed, is whether the offender's act caused annoyance, irritation,

196. *Id*. art. 287.

197. Sy v. Secretary of Justice, 511 SCRA 92, 97 (2006); People v. Villamar 298 SCRA 398, 405 (1998); People v. Astorga, 283 SCRA 420, 439-40 (1997). *See also* REYES, BOOK TWO, *supra* note 143, at 586.

198. BOADO, *supra* note 146, at 692.

199. REYES, BOOK TWO, *supra* note 143, at 591-92 (citing People v. Romero, et al., 44 O.G. 4424 (Court of Appeals)).

200. BOADO, *supra* note 146, at 692.

201. REYES, BOOK TWO, *supra* note 143, at 597.

202. Maderazo v. People, 503 SCRA 234, 247 (2006). *See also* REYES, BOOK TWO, *supra* note 143, at 599.

vexation, torment, distress or disturbance to the mind of the person to whom it is directed."[203]

Based on the preceding discussion of grave coercion and unjust vexation, it would seem that cyberstalking may fall under unjust vexation, but not under grave coercion. While cyberstalking may involve the prevention or compulsion of another to do something through violence, threat, or intimidation, there is no immediacy, actuality, or imminence. More importantly, cyberstalking is not committed directly, but through the use of electronic communication devices. As previously discussed, for a person to be liable under grave coercion, the violence, threat, or intimidation must not be made through an intermediary or in writing, and must be immediate, actual, or imminent. The use of electronic communication devices negates immediacy, actuality, and imminence.

Another reason why grave coercion does not apply to cyberstalking is because not all forms of cyberstalking involve violence, threats, or intimidation. Cyberstalking may be made through online impersonation of a victim or by posting private and personal details of a victim on an online bulletin board. These actions may terrorize a victim despite the absence of violence, threat, or intimidation.

Cyberstalking may fall under the second paragraph of Article 287, or unjust vexation. Certainly, online impersonation of a person or the posting of personal information of another for public viewing may constitute *annoyance, irritation, vexation, torment, distress, or disturbance*. Be that as it may, unjust vexation seems to be an insufficient provision, considering that cyberstalking involves a pattern of conduct with the intent of terrorizing, harassing, causing fear, or placing another under surveillance. Clearly, acts committed by a cyberstalker are more than simple annoyance or irritation. These acts result into causing fear and terror upon the victim, for which the penalties of *arresto menor* or a fine ranging from Php5.00 to Php200.00, as provided for by Article 287, seem insufficient. So serious is the crime of real-world stalking that, in fact, the Anti-Violence Against Women and Their Children Act of 2004[204] imposes the penalty of *prision mayor* and a fine of not less than Php100,000.00 but not more than Php300,000.00 for real-world stalkers of women and their children. In addition, those found guilty of real-world stalking under this law must undergo mandatory psychological counseling or psychiatric treatment. There would be a great disparity if

203. Baleros v. People, 513 SCRA 321, 323-24 (2007); *Maderazo*, 503 SCRA at 247 (citing People v. Reyes, 60 Phil. 369 (1934)). *See also* REYES, BOOK TWO, *supra* note 143, at 599.

204. Anti-Violence Against Women and Children Act of 2004, § 6.

cyberstalking was to be punished merely under unjust vexation, providing for a penalty of only *arresto menor*, whereas real-world stalking of women and their children demands a penalty of *prision mayor*. One must note that the Revised Penal Code took effect on 1 January 1932,[205] when computers, much more cyberstalking, were yet non-existent. The Supreme Court has also ruled that

> [t]he main purpose of the law penalizing coercion and unjust vexation is precisely to enforce the principle that no person may take the law into his hands and that our government is one of law, not of men. It is unlawful for any person to take into his own hands the administration of justice.[206]

In fine, there is no definite law that penalizes cyberstalking. Clearly, the e-Commerce Act of 2000 and grave coercions are not applicable. While the Anti-Violence Against Women and their Children Act of 2004, the Anti-Sexual Harassment Act of 1995, grave or light threats, and unjust vexation may find some applicability in dealing with cyberstalking, they were clearly shown to be insufficient for they do not cover all forms and elements of cyberstalking.

## IV. FOREIGN LAWS

### *A. An Overview of Foreign Laws*

Various cybercrime legislation have been enacted across the globe through the years. Some laws have been in existence since the beginnings of the Internet, such as the Computer Fraud and Abuse Act of the United States,[207] which was enacted by the United States Congress in 1986, while other laws are more recent, including the Philippines' own e-Commerce Act of 2000. Yet still, other laws have recently been revamped to keep up with the changing times, such as the Computer Misuse Act of the United Kingdom.[208]

This Section will discuss various laws from different countries in relation to the cybercrime being studied, to learn from the various intricacies of these different laws, and perhaps apply them to the Philippine setting. The foreign laws that will be discussed are those from the United States, the United Kingdom, as well as the Convention on Cybercrime of the Council of

205. REYES, BOOK ONE, *supra* note 6, at 20-21.

206. *Maderazo*, 503 SCRA at 247-48.

207. Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (1986) (amended in 1994 and 1996).

208. Computer Misuse Act, 1990, c.18 (Eng.).

Europe. This Section is organized according to the type of cybercrime and the various foreign laws applicable to that specific cybercrime.

*B. Phishing*

As phishing has dramatically risen only in the recent years,[209] it has only recently been given much attention by legislators. As of the time of this writing, for example, the United States has not passed any federal law criminalizing phishing, although a bill has been introduced in Congress.[210] As a result, individual states have had to rely on enacting their own legislation to deal with phishing. California was the first state to spell out penalties for Internet fraudsters who steal identities.[211] It passed the Anti-Phishing Law of 2005, which provides:

> 22948.2. It shall be unlawful for any person, by means of a Web page, electronic mail message, or otherwise through use of the Internet, to solicit, request, or take any action to induce another person to provide identifying information by representing itself to be a business without the authority or approval of the business.[212]

Under the said state law, the action may be brought by an individual who is adversely affected; by an internet service provider, a person who owns a website or owns a trademark, who is adversely affected; or by the Attorney General.[213] It defines identifying information by making an enumeration, to wit:

> (b) "Identifying information" means, with respect to an individual, any of the following:
>
> (a) Social security number.

---

209. Robert Louis B. Stevenson, *Plugging the "Phishing" Hole: Legislation versus Technology*, 2005 DUKE L. & TECH. REV. 0006, *available at* http://www.law.duke.edu/journals/dltr/articles/2005dltr0006.html (last accessed Aug. 19, 2008).

210. Internet Business Law Services (IBLS) Editorial Staff, *INTERNET LAW — Are the United States Federal and State Governments ready to Prosecute Phishing Attacks?*, IBLS INTERNET LAW – NEWS PORTAL, Apr. 16, 2007, *available at* http://www.ibls.com/internet_law_news_portal_view.aspx?s=latestnews&id=1731 (last accessed Aug. 19, 2008).

211. Gregg Keizer, *California Enacts Tough Anti-Phishing Law*, INFORMATION WEEK, Oct. 3, 2005, *available at* http://www.informationweek.com/story/showArticle.jhtml?articleID=171202672 (last accessed Aug. 19, 2008).

212. CAL. BUS. & PROF. CODE, § 22948.2 (1997 & Supp. 2006).

213. *Id.* § 22948.3.

(b) Driver's license number.

(c) Bank account number.

(d) Credit card or debit card number.

(e) Personal identification number.

(f) Automated or electronic signature.

(g) Unique biometric data.

(h) Account password.

(i) Any other piece of information that can be used to access an individual's financial accounts or to obtain goods or services.[214]

Although many of these enumerated items may be classified as access devices (as in the Philippine Access Devices Regulation Act of 1998), not all of them necessarily are, such as unique biometric data, social security number, and driver's license number. As can be seen, the main focus of this law is to penalize anyone who induces another to provide him with identifying information through misrepresentation.

The United Kingdom has recently updated its laws by enacting the Fraud Act of 2006[215] which came to effect only on 15 January 2007. This law potentially punishes phishing for up to ten years imprisonment. It provides thus:

2. Fraud by false representation

(1) A person is in breach of this section if he —

(a) dishonestly makes a false representation, and

(b) intends, by making the representation —

(i) to make a gain for himself or another, or

(ii) to cause loss to another or to expose another to a risk of loss

(2) A representation is false if —

(a) it is untrue or misleading, and

(b) the person making it knows that it is, or might be, untrue or misleading.

214. *Id.* § 22948.1 (b).

215. Fraud Act 2006 (Commencement) Order, 2006, S.I. No. 2006/3200, c. 112 (Eng.).

(3) "Representation" means any representation as to fact or law, including a representation as to the state of mind of —

(a) the person making the representation, or

(b) any other person.[216]

While this law is not limited to computer fraud, it definitely covers phishing. "'This reform is needed to enable prosecutors to get to grips with the increasing abuse of technology, particularly in relation to fake credit card scams and *personal identity theft*, which cost millions of pounds every year,' commented Attorney General Lord Goldsmith, the Government's most senior law official."[217] It was noted in a Law Commission report — which influenced the legislation — that prosecutors "were often confused about which law should be applied to which offence"[218] and that "*it was proving difficult to charge a defendant with having committed a crime when it could not be proved that a specific benefit, such as money, had been gained*."[219] In comparison to the Access Device Regulation Act of 1998 of the Philippines, an explanatory note of United Kingdom's Fraud Act 2006 clarifies that subsection (1) (b) does not require gain or loss to have to take place.[220] The Access Device Regulation Act of 1998 specifically requires *production, usage, or traffic* of the access device, or the disclosure of information on an access device, or the obtainment of money or anything of value.[221]

Subsection (4) of the Fraud Act 2006 provides that the representation may be express or implied. The same explanatory note provides that "there is no limitation on the way in which the representation must be expressed," so much so that it definitely covers representations in e-mails and websites.[222] It further and more specifically specifies that the law covers phishing.[223]

---

216. Fraud Act, 2006, c. 35 (Eng.).

217. John E. Dunn, *UK anti-phishing laws given bigger teeth*, TECHWORLD, May 27, 2005, *available at* http://www.techworld.com/security/news/index.cfm?NewsID=3753 (last accessed Aug. 20, 2008) (emphasis supplied).

218. *Id.*

219. *Id.* (emphasis supplied).

220. Fraud Act, 2006, Explanatory Notes, § 2, ¶ 11.

221. Access Devices Regulation Act of 1998, § 9.

222. Fraud Act, 2006, Explanatory Notes, § 2, ¶ 14.

223. *Id.*

The Convention on Cybercrime of the Council of Europe, which took effect on 1 July 2004,[224] has its own provision on computer-related fraud. Although this treaty is not domestic law, it requires signatories to it to legislate laws pertaining to cybercrime. It provides:

> Article 8 — Computer-related fraud
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:
>
> (a) any input, alteration, deletion or suppression of computer data,
>
> (b) any interference with the functioning of a computer system,
>
> with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.[225]

An examination of this provision as well as of the explanatory note reveals that it does not take into consideration phishing, perhaps because phishing has only recently increased in incidence.[226] Furthermore, it can be seen that this provision requires a loss of property. As aforementioned, while phishing may lead to a loss of property, the act of phishing itself does not involve the loss of property, but the theft of personally identifying information. One would be hard pressed to legally consider personally identifying information as property.

### *C. Denial of Service*

While the Convention on Cybercrime of the Council of Europe does not have specific provisions on phishing, it does have provisions on denial of service. It provides:

> Article 5 — System interference
>
> Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.[227]

---

224. Council of Europe, Convention on Cybercrime, *available at* http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=9/2/2006&CL=ENG (last accessed Aug. 20, 2008).

225. Convention on Cybercrime, *supra* note 17, art. 8.

226. *Id.* Explanatory Note.

227. *Id.* art. 5.

The explanatory note of the Convention elucidates that this article requires serious hindering, but leaves to the party-signatories to determine what would constitute as serious hindering. The note, however, specifically gave denial of service attacks as an example of serious hindering.[228] It further mentions that "the drafters considered as 'serious' the sending of data to a particular system in such a form, size, or frequency that it has a significant detrimental effect on the ability of the owner or operator to use the system, or to communicate with other systems."[229] Of course, the serious hindering must be *without right*, as some forms of serious hindering may be legitimate or with authority from the owner or operator of the system.[230] An important facet of this article is that it is technologically neutral so that it could be more prospective. Further, by being neutrally worded, all kinds of functions may be covered by it.[231]

In the United States, a victim of denial of service attacks may pursue legal action under the Electronic Communications Privacy Act.[232] The law punishes "whoever (1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or *prevents authorized access* to a wire or electronic communication while it is in electronic storage in such system."[233] This law provides for a punishment of a fine or imprisonment of not more than five years for the first offense, and not more than 10 years for subsequent offenses, or both, if the denial of service attack is committed for commercial advantage, private commercial gain, or in furtherance of any criminal or tortuous act in violation of the Constitution or laws of the United States.[234] In other instances, the law provides for a punishment of a fine or imprisonment of not more than one year for the first offense, and not more than five years for subsequent offenses, or both.[235]

228. *Id.* Explanatory Note.

229. *Id.*

230. *Id.*

231. Convention on Cybercrime, *supra* note 17, Explanatory Note.

232. Jenevra Georgini & John M. Mrsich, *Terms you need to know: Denial of Service Attacks*, 4 NO. 5 NMEDWST 3 (1998).

233. 18 U.S.C. § 2701.

234. *Id.* § 2701 (b) (1).

235. *Id.* § 2701 (b) (2).

In the United Kingdom, the Computer Misuse Act 1990 has recently been amended by the Police and Justice Act 2006[236] to include denial of service attacks.[237] The Computer Misuse Act 1990 (C.M.A.) was the primary cybercrime legislation of the United Kingdom, and was enacted even before widespread use of the Internet began.[238] The Police and Justice Act 2006, which gained Royal Assent on 8 November 2006, amended the C.M.A. to remove some loopholes when prosecuting denial of service attackers.[239] The amended Section 3 of the C.M.A. provides in part:

> 3. Unauthorised acts with intent to impair, or with recklessness as to impairing, operation of computer, etc.
>
> (1) A person is guilty of an offence if —
>
> (a) he does any unauthorised act in relation to a computer;
>
> (b) at the time when he does the act he knows that it is unauthorised; and
>
> (c) either subsection (2) or subsection (3) below applies.
>
> (2) This subsection applies if the person intends by doing the act —
>
> (a) to impair the operation of any computer;
>
> (b) *to prevent or hinder access to any program or data held in any computer;*
>
> (c) to impair the operation of any such program or the reliability of any such data; or
>
> (d) to enable any of the things mentioned in paragraphs (a) to (c) above to be done.[240]

The amended law provides for a penalty of imprisonment of up to 10 years.[241] The wording of the law is also broad enough to include those people who might pay others to launch an attack.[242]

---

236. Police and Justice Act, 2006, c. 48 (Eng.).

237. Tom Espiner, *U.K. outlaws denial-of-service attacks*, CNET NEWS.COM, Nov. 10, 2006, *available at* http://news.com.com/2100-7348_3-6134472.html (last accessed Aug. 20, 2008).

238. *Id.*

239. Sarah Arnott, *Law cracks down on denial-of-service attacks: Dos attackers now face up to 10 years in prison*, COMPUTING NEWS, Nov. 16, 2006, *available at* http://www.computing.co.uk/computing/news/2168706/law-cracks-denial-service (last accessed Aug. 20, 2008).

240. Police and Justice Act, c. 48, § 36 (emphasis supplied).

*D. Cyberstalking*

The United Kingdom of Great Britain and Northern Ireland also updated their laws with regard to cyberstalking. In 2001, they passed the Criminal Justice and Police Act[243] which amended the Malicious Communications Act 1988[244] to include cyberstalking. The amended act provides as follows:

> 1. (1) Any person who sends to another person —
>
> (a) a letter, *electronic communication* or article of any description which conveys —
>
> (i) a message which is indecent or grossly offensive;
>
> (ii) a threat; or
>
> (iii) information which is false and known or believed to be false by the sender; or
>
> (b) any article or *electronic communication* which is, in whole or part, of an indecent or grossly offensive nature,
>
> is guilty of an offence if his purpose, or one of his purposes, in sending it is that it should, so far as falling within paragraph (a) or (b) above, *cause distress or anxiety* to the recipient or to any other person to whom he intends that it or its contents or nature should be communicated.[245]

The law further defines electronic communication, to wit:

> (2A) In this section "electronic communication" includes —
>
> (a) any oral or other communication by means of a telecommunication system (within the meaning of the Telecommunications Act 1984 (c. 12)); and
>
> (b) any communication (however sent) that is in electronic form.

The penalty is imprisonment not exceeding six months, or a fine, or both.

As the above law is concerned only with communications, it does not clearly cover all forms of cyberstalking, such as harassment by means of impersonation or by posting a victim's address and contact information on an online bulletin board and encouraging third parties to contact, visit, or

---

241. *Id.* § 36.

242. *UK bans denial of service attacks*, OUTLAW.COM, Sep. 11, 2006, *available at* http://www.out-law.com/page-7462 (last accessed Aug. 20, 2008).

243. Criminal Justice and Police Act, 2001, c. 16 (Eng.).

244. Malicious Communications Act, 1988, c. 27 (Eng.).

245. *Id.* c. 27, § 1 (emphasis supplied).

otherwise harass him or her. Thus, the above law is supplemented by the Protection from Harassment Act 1997.[246] It provides:

> 1. (1) A person must not pursue a course of conduct —
>
> (a) which amounts to harassment of another, and
>
> (b) which he knows or ought to know amounts to harassment of the other.
>
> (2) For the purposes of this section, the person whose course of conduct is in question ought to know that it amounts to harassment of another if a reasonable person in possession of the same information would think the course of conduct amounted to harassment of the other.
>
> …
>
> 4. (1) A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.
>
> (2) For the purposes of this section, the person whose course of conduct is in question ought to know that it will cause another to fear that violence will be used against him on any occasion if a reasonable person in possession of the same information would think the course of conduct would cause the other so to fear on that occasion.[247]

These two laws combined sufficiently cover cyberstalking offenses in the United Kingdom.

Cyberstalking laws in the United States are more fragmented than those of the United Kingdom. California, the first state to enact anti-stalking laws, has only recently amended its laws to cover cyberstalking.[248] Specifically, Sections 422, 646.9, and 653m of the California Penal Code were amended to address the problem. Section 422 provides:

> 422. Any person who willfully *threatens* to commit a crime which will result in death or great bodily injury to another person, with the specific intent that the statement, made verbally, in writing, *or by means of an electronic communication device*, is to be taken as a threat, even if there is no intent of actually carrying it out, which, on its face and under the circumstances in which it is made, is so unequivocal, unconditional, immediate, and specific

246. Protection from Harassment Act, 1997, c. 40 (Eng.).

247. *Id.* c. 40, §§ 1 & 4.

248. Attorney General of the United States, STALKING AND DOMESTIC VIOLENCE — REPORT TO CONGRESS 10 (2001) [hereinafter U.S. ATTORNEY GENERAL, STALKING].

> as to convey to the person threatened, a gravity of purpose and an immediate prospect of execution of the threat, and thereby causes that person reasonably to be in sustained fear for his or her own safety or for his or her immediate family's safety, shall be punished by imprisonment in the county jail not to exceed one year, or by imprisonment in the state prison.
>
> For the purposes of this section, "immediate family" means any spouse, whether by marriage or not, parent, child, any person related by consanguinity or affinity within the second degree, or any other person who regularly resides in the household, or who, within the prior six months, regularly resided in the household.
>
> "Electronic communication device" includes, but is not limited to, telephones, cellular telephones, computers, video recorders, fax machines, or pagers. "Electronic communication" has the same meaning as the term defined in Subsection 12 of Section 2510 of Title 18 of the United States Code.[249]

This provision, however, deals solely with threats made through electronic communication devices. Section 646.9 addresses harassment as a form of cyberstalking. The pertinent portions of Section 646.9 are as follows:

> 646.9. (a) Any person who willfully, maliciously, and repeatedly *follows* or willfully and maliciously *harasses* another person and who makes a credible threat with the intent to place that person in reasonable fear for his or her safety, or the safety of his or her immediate family is guilty of the crime of stalking, punishable by imprisonment in a county jail for not more than one year, or by a fine of not more than one thousand dollars ($1,000), or by both that fine and imprisonment, or by imprisonment in the state prison.
>
> . . .
>
> (e) For the purposes of this section, 'harasses' means engages in a knowing and willful course of conduct directed at a specific person that seriously alarms, annoys, torments, or terrorizes the person, and that serves no legitimate purpose.
>
> (f) For the purposes of this section, "course of conduct" means two or more acts occurring over a period of time, however short, evidencing a continuity of purpose. Constitutionally protected activity is not included within the meaning of "course of conduct."
>
> . . .
>
> (h) For purposes of this section, the term "electronic communication device" includes, but is not limited to, telephones, cellular phones, computers, video recorders, fax machines, or pagers. "Electronic

249. CAL. PENAL CODE, § 422 (emphasis supplied).

> communication" has the same meaning as the term defined in Subsection 12 of Section 2510 of Title 18 of the United States Code.[250]

Finally, Section 653m supplements these first two sections as follows:

> 653m. (a) Every person who, with intent to annoy, telephones or makes contact by means of an *electronic communication device* with another and addresses to or about the other person any obscene language or addresses to the other person any threat to inflict injury to the person or property of the person addressed or any member of his or her family, is guilty of a misdemeanor. Nothing in this subdivision shall apply to telephone calls or electronic contacts made in good faith.
>
> (b) Every person who makes repeated telephone calls or makes repeated contact by means of *an electronic communication device* with intent to annoy another person at his or her residence, is, whether or not conversation ensues from making the telephone call or electronic contact, guilty of a misdemeanor. Nothing in this subdivision shall apply to telephone calls or electronic contacts made in good faith.
>
> …
>
> (d) Any offense committed by use of a telephone may be deemed to have been committed where the telephone call or calls were made or received. *Any offense committed by use of an electronic communication device or medium, including the Internet, may be deemed to have been committed when the electronic communication or communications were originally sent or first viewed by the recipient.*[251]

At the federal level, the United States has the Interstate Communications law, which makes punishable the transmission of threats to injure another person.[252] The pertinent parts of the law state:

> (b) Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than twenty years, or both.
>
> (c) Whoever transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both.

250. *Id.* § 646.9 (emphasis supplied).

251. *Id.* § 653m (emphasis supplied).

252. U.S. ATTORNEY GENERAL, STALKING, *supra* note 248, at 15.

> (d) Whoever, with intent to extort from any person, firm, association, or corporation, any money or other thing of value, transmits in interstate or foreign commerce any communication containing any threat to injure the property or reputation of the addressee or of another or the reputation of a deceased person or any threat to accuse the addressee or any other person of a crime, shall be fined under this title or imprisoned not more than two years, or both.[253]

The limitation of this law, however, is the fact that it applies only to threats, and not to other forms of cyberstalking such as harassment, or the posting of messages in an online bulletin board encouraging third parties to harass the victim.[254]

Another federal law designed to curb cyberstalking is Section 223 of Title 47 or the Communications Act of 1934 as amended by the recently reauthorized Violence Against Women Act of 2005. It provides:

> (a) Prohibited acts generally
>
> Whoever —
>
> (1) in interstate or foreign communications —
>
> …
>
> (C) makes a telephone call or utilizes a telecommunications device, whether or not conversation or communication ensues, without disclosing his identity and with intent to annoy, abuse, threaten, or harass any person at the called number or who receives the communications;
>
> (h) Definitions
>
> For purposes of this section —
>
> (1) The use of the term "telecommunications device" in this section —
>
> …
>
> (C) in the case of subparagraph (C) of subsection (a)(1), includes any device or software that can be used to originate telecommunications or other types of communications that are transmitted, in whole or in part, by the Internet (as such term is defined in section 1104 of the Internet Tax Freedom Act (47 U.S.C. 151 note)).[255]

---

253. 18 U.S.C. § 875.

254. U.S. ATTORNEY GENERAL, STALKING, *supra* note 248, at 17.

255. 47 U.S.C. § 223, *amended by* Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. No. 109-162, 119 Stat. 2960.

The Violence Against Women Act of 2005, under its Section 113, entitled Preventing Cyberstalking, specifically provided for the addition of paragraph (C) under the section 223 (h) (1) to include Internet communications in Section 223 (a) (1), paragraph (C). It provides for a penalty of a fine or imprisonment of not more than two years or both.[256] The insufficiency of this law in relation to cyberstalking is that it applies only to direct communications, leaving out harassment made through posting messages on online bulletin boards and websites, inviting third parties to harass or terrorize the victim. Furthermore, the said provision is only a misdemeanor with a penalty of not more than two years.[257]

Yet another federal law, the Interstate Stalking Law, also covers cyberstalking. It provides:

> § 2261A. Interstate stalking
>
> Whoever —
>
> …
>
> (2) with the intent —
>
> …
>
> (B) to place a person in another State or tribal jurisdiction, or within the special maritime and territorial jurisdiction of the United States, in reasonable fear of the death of, or serious bodily injury to —
>
> (i) that person;
>
> (ii) a member of the immediate family (as defined in section 115) of that person; or
>
> (iii) a spouse or intimate partner of that person,
>
> uses the mail or any facility of interstate or foreign commerce to engage in a course of conduct that places that person in reasonable fear of the death of, or serious bodily injury to, any of the persons described in clauses (i) through (iii),
>
> shall be punished as provided in section 2261 (b).[258]

And Section 2261 (b) provides:

> (b) Penalties. — A person who violates this section or section 2261A shall be fined under this title, imprisoned —

256. *Id.* § 223 (a).

257. U.S. ATTORNEY GENERAL, STALKING, *supra* note 248, at 11.

258. 18 U.S.C. § 2261A.

> (1) for life or any term of years, if death of the victim results;
>
> (2) for not more than 20 years if permanent disfigurement or life threatening bodily injury to the victim results;
>
> (3) for not more than 10 years, if serious bodily injury to the victim results or if the offender uses a dangerous weapon during the offense;
>
> (4) as provided for the applicable conduct under chapter 109A if the offense would constitute an offense under chapter 109A (without regard to whether the offense was committed in the special maritime and territorial jurisdiction of the United States or in a Federal prison); and
>
> (5) for not more than 5 years, in any other case, or both fined and imprisoned.[259]

The weakness of this law is that it requires for there to be reasonable fear of death, or serious bodily injury on the part of the victim, or his or her immediate family, or his or her spouse or intimate partner. Cyberstalking does not necessarily require fear of death or serious bodily injury, as all it requires is a pattern of conduct that terrorizes, harasses, threatens, causes fear, or places another under surveillance. Such actions need not amount to a fear of death or bodily injury. A cyberstalker may, for example, post the address and contact details of a victim on a website and encourage others to harass the victim, which does not necessarily amount to fear of death.

*E. Conclusion*

Upon examining these various foreign laws, it can be seen unequivocally that other states have made efforts to ensure that cybercrimes are kept at bay, or at least to hold liable cyber offenders. While there is no unanimity as to the wordings and definitions of these various laws, there is unanimity as to the need to address cyber offenses. As recent as 2005 and 2006, California and the United Kingdom have updated their laws to address phishing. Their laws now cover matters of misrepresentation, taking into consideration the theft of personally identifying information.

As regards denial of service attacks, the United States and the United Kingdom both have laws to tackle the matter. The United Kingdom, in fact, amended its laws, which gained Royal Assent on 8 November 2006, to ensure coverage of denial of service attacks. Denial of service attacks have even been embodied in an international convention designed to deal with cybercrime, the Convention on Cybercrime of the Council of Europe.

---

259. *Id.* § 2261.

On the matter of cyberstalking, several laws have been enacted to hold cyberstalkers liable for their terrorizing acts. Consideration has been made of the fact that cyberstalking may indeed be more terrifying than real-world stalking, given the greater anonymity of cyberstalker. In the United Kingdom, the Criminal Justice and Police Act 2001 was enacted to amend their Malicious Communications Act 1988 to include cyberstalking. The United States as well has several statutes to deal with cyberstalking.

Indeed, these countries cannot be faulted with allowing their laws to fall so far behind.

## V. CONCLUSIONS AND RECOMMENDATIONS

### *A. Conclusions*

An analysis of the applicability of Philippine laws to the cybercrimes of phishing, denial of service, and cyberstalking will reveal their insufficiency. By examining the elements of these crimes in relation to pertinent Philippine laws, it can gleaned that either no law punishes these crimes or there would be great ambiguity as to whether or not these laws would be applicable, to the point of expanding their reach. This results in a void in the law in the event these crimes are committed within Philippine territorial borders. After all, it is a basic tenet in Philippine law that there is no crime when there is no law that incriminates the act,[260] and further, that "penal statutes may not be enlarged by implication or intent beyond the fair meaning of the language used; and may not be held to include offenses other than those which are clearly described."[261] If the love bug tragedy has taught the Philippines anything, it is that it must always adapt its laws to the changing times, and to have sufficient laws to fill-in gaps in the justice system. Computers have indeed been revolutionizing tools of modern society, and have existed as early as the time the author of this Note was born. Yet, it has taken Philippine legislators more than a score to enact legislation to address the growing threats of computer crime (i.e. e-Commerce Act of 2000). This

260. REYES, BOOK ONE, *supra* note 6, at 1; BERNAS, *supra* note 6, at 494 (citing U.S. v. Luling, 34 Phil. 725, 728 (1916)).

> The State having the right to declare what acts are criminal, within certain well defined limitations, has a right to specify what act or acts shall constitute a crime, as well as what proof shall constitute prima facie evidence of guilt, and then to put upon the defendant the burden of showing that such act or acts are innocent and are not committed with any criminal intent or intention.

261. Laurel v. Abrogar, 483 SCRA 243, 267 (2006); Campomanes v. People, 511 SCRA 285, 300 (2006).

begs the question of whether it would take another score to update its laws. The aim of this Note is to determine the sufficiency of Philippine laws to combat emerging trends in cybercrime. It has been determined that there is indeed a lack of legislation. On this premise, new legislation must be enacted if the Philippines is to learn from its lessons.

An examination of foreign laws will show that these crimes have been addressed by more progressive countries. The United States and the United Kingdom, for example, have made laws addressing denial of service attacks and cyberstalking. Most states of the United States have laws on phishing, and cyberstalking. The European Union, through the Council of Europe, and in conjunction with their partners — Canada, Japan, South Africa, and the United States — have banded together to formulate the Convention on Cybercrime,[262] "convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, *inter alia*, by adopting appropriate legislation and fostering international co-operation."[263] While the world recognizes the need to legislate against cybercrime, the Philippines appears to have taken a back seat on cybercrime legislation. One must keep in mind, as shown by the love bug virus, that Philippine cyber offenders can cause billions of dollars in damage across the globe, whether the victim country is developed or developing. As cybercrime is borderless, they would have the same elements regardless of the country, as long as that country has computers and access to the Internet. Learning from countries with appropriate cybercrime legislation would save time and money for the Philippines.

### *B. Recommendations*

#### 1. Proposal for New Legislation

New legislation is recommended to specifically address the problem of cybercrime, particularly the crimes of phishing,[264] denial of service,[265] and

262. Convention on Cybercrime, *supra* note 17, Explanatory Note.

263. *Id.* Preamble.

264. *Phishing.* — Any person is guilty of phishing if he, without authority and through false representation, solicits, requests, or otherwise induces another to provide personally identifying information, through the creation of an online site, sending of electronic mail, or otherwise through the use of computer systems, electronic communication devices, or the Internet.

265. *Denial of Service Attack.* — A person is guilty of a denial of service attack if he intentionally, without or in excess of authority, seriously hinders or prevents the legitimate functioning of or access to or from a computer system or electronic communication device or online service; through interference or disruption of

cyberstalking.[266] These acts, their elements as propounded in the previous parts of this Note, must be prohibited and penalized.

Imprisonment should be made mandatory, as with the e-Commerce Act, so as to prevent wealthy cyber offenders from simply paying-off fines and avoiding penalty based on wealth. Instead of a maximum of three years as provided by the e-Commerce Act, the maximum should be increased to 10 years, taking cue from laws of other states.[267] A bill proposed by Senator Ramon B. Magsaysay, Jr. penalizes similar offenses with imprisonment for not less than eight years nor more than 20 years, with a fine ranging from Php100,000.00 or equal in amount to the damage involved in the violation, whichever is applicable.[268] As discussed in the second Section, phishing and denial of service may not necessarily involve damage or prejudice to another that is capable of pecuniary estimation, as what is involved is the theft of personally identifying information or the prevention or hindrance of access to a computer, network, or online service.

Also, presidents, members of the board of directors, employees or officers of juridical entities should be held liable, so that cyber offenders may not hide behind the veil of a corporate entity. Otherwise, this proposed law

---

computer or network communications, through the consumption of computer network resources, or through the alteration of configuration information of a computer or electronic communication device.

266. *Cyberstalking*. — A person is guilty of cyberstalking if he, without lawful justification, engages in a pattern of conduct, such as but not limited to the sending of an online message to another, the online impersonation of another, or the posting online without authority of personal information of another for public viewing, or any use of an electronic communication device, with the intent of terrorizing, harassing, threatening, or otherwise causing fear to another, or placing another under surveillance, or any combination thereof. The person whose pattern of conduct is in question ought to know that it amounts to harassment of another if a reasonable person in possession of the same information would think the pattern of conduct amounted to harassment of another.

267. A violation of phishing and denial of service attack shall be punished by a minimum fine of Php100,000.00 and a maximum of Php300,000.00 or an amount commensurate to the damage incurred, if applicable, and a mandatory imprisonment for not less than four years nor more than 10 years; *Provided*, that if the person violating any provisions of this Act is a juridical person, the penalty herein provided shall be imposed on its president or secretary and/or members of the board of directors or any of its officers and employees who may have directly participated in the violation.

268. Anti-Computer Fraud and Abuses Act of 2004, § 4, S.B. 1789, 13th Cong., 1st Sess. (Sep. 17, 2004).

might be rendered nugatory as cyber offenders may be able to escape liability for committing the abovementioned prohibited acts simply by forming a corporation. This same rationale, however, does not exist for cyberstalking as the offense of cyberstalking is personal in nature.[269] Based on the discussions in the second and third Sections of this Note, only a natural person may commit the offense of cyberstalking.

2. A Comprehensive Bill

While this Note deals with the cybercrimes of phishing, denial of service attacks, and cyberstalking, it would perhaps be more sensible to pass a comprehensive bill that deals with all forms of cybercrime. It is not recommended that piecemeal legislation be adopted as this may cause confusion, particularly to the public who are to abide by these laws and to prosecutors who are already overwhelmed with work. There are undeniably other forms of cybercrime aside from phishing, denial of service attacks, and cyberstalking that must be addressed by the Philippines in this world revolutionized by computers and the Internet. Consequently, the author proposes and advocates the passage of comprehensive anti-cybercrime legislation to handle the various issues concerning computer, network, and Internet security.[270]

*C. Epilogue*

Admittedly, implementation of a cybercrime law may be difficult, considering the limited resources of the government. Nevertheless, the author believes that the mechanisms for the implementation of this law are already available. The Commission on Information and Communication Technology, the Department of Justice, the National Bureau of Investigation, the Prosecutor's Office, as well as the Departments of Trade and Industry and Science and Technology are available at the disposable of the government, and there is no need to create any new agency to implement this law. Moreover, as with other penal laws, private citizens may bring complaints to the prosecutor's office in the event that they become victims of such acts. There is no shortage of hands — and there should not

269. A violation of Section 7 shall be punished by a minimum fine of Php100,000.00 and a maximum of Php300,000.00, and a mandatory imprisonment of not less than four years nor more than 10 years.

270. *See generally* Rosalyn C. Rayco, Cyber Prostitution at a Click of a Button: Evaluating the Applicability of Prostitution Statutes in Criminalizing Paid Video-based Cybersex 117-18 (2006) (unpublished J.D. thesis, Ateneo de Manila University) (on file with the Professional Schools Library, Ateneo de Manila University).

be — in ensuring the information and communication technology growth, safety, and security of the country.

As earlier mentioned, there is a void in the Philippine justice system that must be filled. Enacting a cybercrime law will provide a tool to prosecute cyber offenders, bring justice to those offended, and secure the rights of the Filipino people to the free, legitimate, and proper use of computers, computer networking, electronic communication, and the Internet. Once before, the Philippines was in a precarious situation wherein it did not have enough laws to pursue cyber offenders. Indeed, the country was embarrassed in the world's eyes when one of its citizens was able to cause billions of dollars in damage, and yet the country could not hold him accountable. To save face, it immediately enacted the e-Commerce Act of 2000. It seemed to have stopped there, however. Perhaps Filipinos have forgotten. Or perhaps Filipinos have not realized that laws do not adapt and morph by themselves. This Note has clearly shown that Philippine laws may not stand another test. It does seem farfetched that we may be victims of cybercrime. But perhaps, one ought to consider the amount of time Filipinos use computers and the Internet. One should also consider that anyone who uses a computer would not hesitate in saying that they have been affected by a computer virus at one point or another.

As the world becomes smaller, Filipinos become not only citizens of the Philippines, but citizens of the world. The Philippines participates in a global community, made more concrete by computer connections. One may not realize that we are all taking part in a revolution brought about by computers and networking, wherein mundane tasks involve these machines more and more. From paying one's bills, to transacting at the grocery store, to buying an airplane ticket, to saying hello to a friend on the other side of the globe, it may not be long before society becomes completely and totally dependent on computers. This being so, Filipinos must secure their computer networks, not only for themselves, but also for the rest of the world.