BALANCING OF INTEREST IN THE DIGITAL AGE: PROTECTION OF THE RIGHTS OF OFFENDED PARTIES AND THE CONSTITUTIONAL RIGHTS OF THE ACCUSED IN THE CONTEXT OF SEX SCANDALS *

*Charisse Mae V. Mendoza***

> *"The enjoyment of a private reputation is as much a constitutional right as the possession of life, liberty or property. It is one of those rights necessary to human society that underlie the whole scheme of civilization."*[1]

I. INTRODUCTION: THE HAYDEN KHO SCANDAL

It was May 2009: Sex videos of Hayden Kho, a celebrity doctor previously better known as the lover of Dra. Vicky Belo, one of the country's top cosmetic surgeons, circulated in the Internet and were later sold in the streets and sidewalks along with pirated DVDs. Among the women who were featured in those videos was Katrina Halili, a local actress.

---

* Awardee, Generoso V. Jacinto Best Paper in Remedial Law (2011). *Cite as* Charisse Mae V. Mendoza, *Balancing of Interest in the Digital Age: Protection of Rights of Offended Parties and the Constitutional Rights of the Accused in the Context of Sex Scandals,* 86 PHIL L.J.356, (page cited) (2012).

** Junior Associate, Berberabe Santos & Quiñones Law Firm; B.A. Pol Sci (2006, Cum Laude), University of the Philippines; J.D. (2011), University of the Philippines College of Law.

[1] Worcester v. Ocampo, G.R. No. L-5932, 22 PHIL 42, Feb. 27, 1912.

As with the other victims who made their sides known, Halili allegedly did not consent to taking of the video.[2] She was, however, seen in one of the videos dancing in the tune of "Careless Whisper" with Kho, wherein she seemed to be aware that she was being recorded. Nevertheless, consent or no consent to the recording of the act in video notwithstanding, the distribution of these videos on the Internet and in the black market were all done without the consent of the women featured in the videos.[3]

Halili sought the help of Senator Ramon Revilla. This led to a Senate hearing in aid of legislation. Criminal charges were also filed by Halili against Kho for violation of Republic Act No. 9282 (Anti-Violence Against Women and Children Act).[4]

Reports further came out linking Belo and two other individuals – one Erick Johnston Chua and a certain Mark Herbert Rosario – to the distribution of the videos. Chua allegedly agreed to such instructions as a form of vengeance against Kho because one of the women featured in the videos was Chua's girlfriend. His girlfriend admitted that she had a short affair with Kho.[5]

Belo allegedly ordered the two individuals, both colleagues of Kho in the Belo Medical Group, to retrieve computers owned by her company from Kho's apartment. The computer was password-protected but in one way or another, they were able to open the computer and find the sex videos stored in it. Belo instructed Chua to burn a copy of the videos into a DVD. After copying the videos to the DVD, the files were deleted from Kho's computer.[6]

---

[2] Ginger Conejero, *Hayden seeks dismissal of case filed by Katrina*, *at* http://www.abs-cbnnews.com/entertainment/10/23/10/hayden-seeks-dismissal-case-filed-katrina (last visited Feb. 20, 2011).

[3] Ruben Manahan, *Halili seeks NBI help; Kho faces sanctions*, THE MANILA TIMES, May 21, 2009, *available at* http://archives.manilatimes.net/national/2009/may/21/yehey/metro/20090521met1.html (last visited Nov. 28, 2010).

[4] Dona Pazzibugan, *Cosmetic doctor charged for secretly filming sex videos*, PHIL. DAILY INQUIRER, Oct. 22, 2009, *available at* http://newsinfo.inquirer.net/inquirerheadlines/metro/view/20091022-231706/Cosmetic-doctor-charged-for-secretly-filming-sex-videos (last visited Nov, 29, 2010).

[5] Bong Godinez, *PART II: Hayden Kho's camp points to Erik Chua as likely sex-video source*, *at* http://www.pep.ph/features/controversies/19176/part-ii-hayden-khos-camp-points-to-erik-chua-as-likely-sex-video-source/1 (last visited Feb. 20, 2011).

[6] Bong Godinez, *Erik Johnston Chua submits court affidavit denying involvement in spread of Hayden's sex videos*, *at* http://www.pep.ph/features/controversies/19271/erik-johnston-

Then after watching the videos in the DVD, Belo allegedly destroyed her copy.[7]

Criminal charges were similarly filed against Belo, Chua and Rosario but these were later dropped by the Department of Justice for insufficiency of evidence.[8]

In a follow up operation, the agents of the National Bureau of Investigation raided the office of the website which was traced to be the first to upload the sex videos of Kho.[9] The said individuals were subsequently charged with violation of Article 201 of the Revised Penal Code.[10]

As of December 2010, the charges against Kho were all dismissed when his Motion for Demurrer to Evidence was granted. The lower court found that evidence was insufficient to convict Kho with violation of Republic Act 9262 or the Anti-Violence Against Women and their Children Act of 2004. This was primarily because of Halili's admission during the Senate hearing that she consented to Kho's taking of three prior video recordings showing that she and the accused together performing salacious acts. The court found that these videos "clearly indicated that she agreed to the taking, or at the very least knew, of the [subject sex] video recording." Further, the lower court found that the location of the camera was in an open and unconcealed place and cannot escape unnoticed. The court found the evidence insufficient to prove that the sex video was taken without Halili's knowledge.[11] Halili's side planned to appeal in order to recover civil damages against Kho.[12]

---

chua-submits-court-affidavit-denying-involvement-in-spread-of-haydens-sex-videos/1/1 (last visited Feb. 20, 2011).

[7] Elyas Isabelo Salanga, *Dr. Vicki Belo's sworn affidavit narrates details of how she destroyed Hayden Kho's sex videos*, *available at* http://www.pep.ph/features/controversies/19276/dr-vicki-belos-sworn-affidavit-narrates-details-of-how-she-destroyednbsp-hayden-khos-sex-videos/4/1 (last visited Feb. 20, 2011).

[8] Dona Pazzibugan, *supra* note 3.

[9] GMANews.TV, *NBI raids website that first uploaded Hayden sex video*, *at* http://www.gmanews.tv/story/166541/NBI-raids-website-that-first-uploaded-Hayden-sex-video (last visited Feb. 20, 2011).

[10] abs-cbnNEWS.com, *Owners of Hayden sex video website sued*, *at* http://www.abs-cbnnews.com/nation/metro-manila/07/06/09/owners-hayden-sex-video-website-sued (last visited Feb. 19, 2011).

[11] Non Alquitran, *Hayden Kho cleared on sex video charges*, PHIL. STAR, Dec. 14, 2010, *available at*

Halili is not alone in this battle. Unfortunately, many women and children, as well as men, had photographs and videos of them in compromising positions taken and posted on the internet with or without their consent (situations which may fall under the term "sex scandal"). Sex scandals are "the highest form of invasion to the privacy of the offended party, most of whom are women".[13] The "main actors" of these offenses forever suffer social stigma, to the extent that some resorted to take their own lives in humiliation. In September 2010, an 18-year old college freshman videotaped of having sex with another male, committed suicide. His roommates allegedly secretly recorded the said acts and broadcasted the images via an internet chat program[14]. The psychological trauma and the judgment of the society would forever damage the lives of these victims, especially in cases of Filipino women who are often described in Jurisprudence as by nature shy, bashful and coy.[15]

This paper aims to present the problems and issues faced in the prosecution of sex scandals in the light of advancements in technology.

The first part of the paper would describe how the improvements in technology create new forms of crimes (what are coined as "cybercrimes"), particularly sex scandals, and would examine whether our country has already provided laws which punish such offenses.

Next, the paper would describe the issues with regard the discovery and presentation of evidence in relation to this crime, and review the rules applicable in the country. In the course of the discussion, the author would try to outline the problems faced by law enforcement officers in the discovery of

---

http://www.philstar.com/Article.aspx?articleId=639188&publicationSubCategoryId=200 (last visited Feb. 20, 2011).

[12] Mike Frialde, *Lawyer predicts CA will overturn Hayden's acquittal*, PHIL. STAR, Dec. 19, 2010, *available at* http://www.philstar.com/Article.aspx?articleid=640569 (last visited Feb. 20, 2011).

[13] Sandra Araneta, *Kho, Belo summoned over Katrina sex video,* PHIL. STAR, May 22 2009, *at* http://www.philstar.com/Article.aspx?articleId=470134 (last visited Feb. 20, 2011).

[14] The Associated Press, *New Jersey student's suicide after secret sex tape illustrates Internet dangers,* *at* http://www.nola.com/crime/index.ssf/2010/09/new_jersey_students_suicide_af.html, (last visited Feb. 20, 2011).

[15] People v. Faigano, G.R. No. 113483, 22 February 1996; Jimenez v. Izares, G.R. No. L-12790, August 31, 1960.

evidence involved in sex scandals, particularly those involving the right of the accused to privacy and against unreasonable searches and seizure.

In line with the right of the accused to be presumed innocent until proven otherwise,[16] it is a common principle in law and jurisprudence that it is better to acquit a man upon the ground of reasonable doubt, even though he may in reality be guilty, than to confine in the penitentiary for the rest of his natural life a person who may be innocent.[17] Thus, his rights should also be sufficiently protected even to the extent of sustaining his innocence and losing the case, and the paper aims to test whether his rights are sufficiently safeguarded by the laws of our country.

The paper would then assess whether the existing laws in the country sufficiently address the problems earlier emphasized, and examine the efforts made by our Legislature and our Judiciary to address such problems. In the end, the author would try to show that even if we do have existing laws to prosecute cybercrimes and address the other issues at hand, it would be better to create new laws and rules more apt to the developments in criminal prosecution brought about by advancements in technology.

The author would try to refer to incidents in sex scandals, factual or imagined, during the course of the paper to make it easier for the readers to contextualize the discussion that would follow below.

II. CRIMES IN THE DIGITAL AGE

It cannot be denied that the use of computers is becoming prevalent in our present generation. More and more information are created, exchanged, and stored in digital form. Various activities can now be done with the use of computers and the aid of Internet. Committing a crime is one of them.

The development of the Internet and the proliferation of computer technology have created new opportunities for those who would engage in illegal activity. The rise of technology and online communication has not only produced a dramatic increase in the incidence of crimes, it has also resulted in

---

[16] CONST. art. III, §14(2); RULES OF COURT, Rule 115, §1(a), Rule 131, §3(a), and Rule 133, §2.

[17] People v. Cawili, G.R. No. L-30543, July 15, 1975, *citing* People v. Manoji, G.R. No. 46412, September 18, 1939.

the emergence of what appear to be some new varieties of it. Both the increase in the incidence of criminal activity and the possible emergence of new varieties of criminal activity pose challenges for legal systems, as well as for law enforcement.[18]

A. Cybercrime and the Carter Classification

The term "cybercrime" has not been formally defined in jurisprudence. There were, however, efforts to classify these crimes, the most famous of which was that made by Professor David Carter.[19] Carter classified computer crimes into four categories (henceforth coined as the "Carter Classification"): (1) where the computers are target of the criminal act itself; (2) where the computers are the instrumentality of the crime; (3) where computers are incidental to the crime; and (4) where the crime is enhanced by computers.

1. Computers as Targets

Computers are treated as targets in two instances: when the object of the crime is to damage the computer itself, or second, when the object is to access the computer and the data it contains without the consent of the owner of the computer.

Examples of crimes wherein computers are the targets are as follows: (1) illegal access, such as hacking, cracking, and computer trespass; (2) illegal interception, such as the use of electronic eavesdropping devices in obtaining data; (3) system interference, such as virus dissemination and denial-of-service attacks; and (4) data interference, such as the use of malicious codes to modify data in the computer.[20]

---

[18] Susan W. Brenner 'Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law' 8 Murdoch University Electronic Journal 2 (2001) *available at* <http://www.murdoch.edu.au/elaw/issues/v8n2/brenner82_text.html>.

[19] David L. Carter, Computer Crime Categories: How Computer Criminals Operate, The FBI Magazine, July 1995, *available at* http://www.lectlaw.com/files/cri14.htm (last visited Jul. 30, 2010).

[20] Rodolfo Noel S. Quimbo, *Cybercrime and Security Policy Issues , power point presentation prepared for Information, Communication and Space Technology Division*, UNESCAP *available at* http://www.authorstream.com/Presentation/GenX-57138-08-Cybercrime-Security-Policy-Issues-Cyber-crime-Two-Part-Presentation-a-Entertainment-ppt-powerpoint/ (last visited Jul. 30, 2010)

2. Computers as Instrumentality of the Crime

With the creation of computers and the Internet, criminals now have new means of committing crimes. When a computer hardware has played a significant role in a crime, it is considered an instrumentality. The clearest example of a computer used as an instrumentality of crime is a hardware that is specially manufactured, equipped and/or configured to commit a specific crime. For instance, sniffers are pieces of hardware that are specifically designed to eavesdrop on a network. Computer intruders often use sniffers to collect passwords that can be used to gain unauthorized access to computers.[21]

Under the Budapest Convention on Cybercrimes, the following are offenses wherein computers or other electronic devices are used as instrumentality of crimes: (1) the use, production, sale, procurement, importation, distribution, and even possession of any device primarily designed/adapted primarily for committing crimes wherein the computer is the target[22]; (2) the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data, otherwise known as computer forgery;[23] (3) intentional or unauthorized input, alteration, suppression of computer data with intent of procuring for economic benefit for one self or for another, otherwise known as computer fraud;[24] and (4) producing, offering, making, distributing, transmitting, procuring through a computer system, or possessing on a computer system child pornography.[25]

a. Computers as incidents of the crime

Although there seems to be little difference between computers being used as instruments in the crime and computers as incidents of the crime, under this classification, the computer is not the primary tool for which the crime may be committed. It is not indispensable to the commission of the crime, but only facilitates its commission.

---

[21] Eogan Casey, DIGITAL EVIDENCE AND COMPUTER CRIME: FORENSIC SCIENCE, COMPUTERS AND THE INTERNET 36 (2004).

[22] Budapest Convention on Cybercrimes, Nov. 23, 2001, §6, *available at* http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm.

[23] *Id.*, §7.

[24] *Id.*, §8.

[25] *Id.*, §9.

Examples of crimes wherein computers serve as incidents of the crime are cyberstalking, drug trafficking, money laundering, and pornography.[26] Many of the new forms of crimes created with the advances in technology and the Internet are merely facilitated by computers.

b. Crimes enhanced by computers

Although these crimes may also fall under the second or third category, a separate classification was deemed proper for these types of crimes as these are crimes which are already prevalent with previously existing technological developments, but with the aid of computers, the perpetration of these crimes became easier and faster.

Examples of crimes considered to be classified under this category are the software piracy and copyright infringement.[27]

B. Sex Scandals as Cybercrimes

Based on the Carter Classification, we can define "cybercrimes" as simply the exploitation of a new technology to commit old crimes in new ways and, concededly, to engage in a limited variety of "new" types of criminal activity.[28] It is the term that collectively refers to crimes which are brought upon by the advancement of technology, particularly with the aid of or through the use of the Internet and computers. It is thus essential to define what computers are.

Under the E-Commerce Act of 2000[29] and the Rules on Electronic Evidence[30], a "computer" refers to any single or interconnected device or apparatus which by electronic, electro-mechanical, optical, and or magnetic impulse, or any other means with the same function, can receive, record, transmit, store, process, correlate, analyze, project, retrieve and/or produce information, data, text, graphics, figures, voice, video, symbols or other modes of expression or perform any one or more of these functions. The definition is likewise broad enough to include all types of electronic equipment including

---

[26] See also Rodolfo Noel S. Quimbo, *supra* note 19.

[27] *Id.*

[28] Brenner, *supra* note 17.

[29] Rep. Act. No. 8792, § 6(c) (2000). This is the E-Commerce Act of 2000.

[30] A.M. No. 01-7-01-SC, Rule 2, §1(d) (2001). This is the Rules on Electronic Evidence.

desktop and mobile computers, fax machines, scanners, printers, computer monitors, card readers, smart cards, credit cards, ATM cards, mobile phones, pagers, radios, VCRs, video equipment, audio equipment, personal digital assistants ("PDAs"), answering machines and telephones.[31]

The individual acts committed to come up with sex scandals are considered cybercrimes. In the Philippine context, the term "sex scandal" is usually associated to videos and images clandestinely acquired either of famous or even ordinary persons. What is necessary to constitute such videos as being sexually scandalous is that the actors therein are not aware that their acts are being caught on tape, or that the actors therein intended that the video or images being generated remain for the personal consumption of the actor's (or their better halves) and not for the public. However, these videos eventually leaked and were shown in the Internet.[32]

There are at least three stages in the commission of a sex scandal. The first stage or set of offenses involves the recording of the video or taking of a picture of persons engaged in sexual activity or compromising positions, with or without their knowledge. Second is the copying of the photo or video from where it was originally stored, again with or without the consent of the persons in it. Third is the distribution and publication of the said photo or video, either by uploading on the Internet, or by reproducing the material, as are seen on the sidewalks of Quiapo (albeit now, with matching title coined by the perverted minds of the DVD vendors). In all these three stages, especially in cases when the persons featured on those videos and photos did not give their consent to any of it, many of the acts done have violated the honor and reputation of the victim of the said scandal. But under our existing laws, can these victims prosecute their offenders and be brought to justice?

C. Katrina's Wrath: Punishing the Perverts

In early May 2000, a computer virus known as the "love bug" emerged and spread rapidly around the globe. The "love bug" forced the shutdown of computers at large corporations. When security and information technology

---

[31] Jesus Disini, Jr. & Janette Toral, *The Electronic Commerce Act and its Implementing Rules and Regulations*, *at* http://www.disini.ph/downloads/EcomIRR%20Annotations.pdf (last visited 24 February 2011).

[32] Ailyn Cortez, et al., A descriptive study on Cybersex, Audio-Visual Sex Scandals, and Child Pornography: Prosecution under existing Philippine Laws, and Other proposals as a framework for future legislation, *at* http://http://berneguerrero.com/node/11 (last visited Feb. 22, 2011).

experts discovered that the virus was created in the Philippines, they were disappointed to find out that the country lacked computer crime laws.[33]

Fast forward nine years after: it was May 2009 when the Hayden Kho-Katrina Halili sex scandal broke out. Would the same case happen to Halili? As was mentioned earlier, Halili filed a complaint for violation of Section 5 of the Anti-Violence against Women and Children Act against Kho. Under the existing laws when Halili filed the complaint, what may be available to Halili as basis for her complaint against the other actors in the controversy?

1. Under the Revised Penal Code

Act No. 3815, or the Revised Penal Code (henceforth RPC), was promulgated way back in 1930, decades before the Internet and computers were even invented. There were cameras back then, but it was not easy to reproduce nor even develop photographs at that time. Video recorders have been invented, but only in the 1950s was a video tape recorder invented by Charles Ginsburg.[34] Clearly, the said law was enacted at a time when sex scandals were unthinkable.

Nevertheless, the RPC would be the first law at which prosecutors would look to determine if the acts involved in sex scandals are punishable in our country.

a. Pornography

Since sex scandals are clearly controversial in a relatively conservative and generally religious country, offenses against decency and good customs would be the first on a prosecutor's list.

Under Article 201 of the RPC (immoral doctrines, obscene publication and exhibitions, and indecent shows), authors of obscene literature, published with their knowledge in any form, the editors who publish such literature, and the owners/operators of the establishment selling the same are liable for a fine ranging from six to twelve thousand, or the penalty of *prision mayor*. Individuals who exhibit indecent shows, understood to mean those which serve no

---

[33] *See* Susan Brenner, *supra* note 17.

[34] *The History of Video and Related Innovations*, *available at* http://inventors.about.com/library/inventors/blvideo.htm (last visited Feb. 25, 2011).

purpose but to satisfy the market for lust or pornography and are contrary to morals and good customs, also suffer the same penalties. Lastly, individuals who sell, give away, or exhibit films or prints are also liable under the said provision.

The offense in any of the forms punishable under the said provision is committed only when there is publicity.[35] In the context of sex scandals, the photographs or videos are uploaded online. Once uploaded, anyone who has access to the website where the photographs or videos are uploaded would be able to view the said material. Publication, as in the context of libel, is the communication of the defamatory matter to some third person or persons.[36] It can therefore be said that a video uploaded online is considered publicity of the photograph or video.

The author of the photograph or video is the one who took it. However, for the said author to be held liable under this provision, he should have knowledge of the publication (i.e. uploading online) of the same.[37]

Unfortunately, in the case of Halili, Kho admitted to the taking of the videos – even claimed that he collected the videos for personal viewing only – but did not admit any liability as to the publication of the video online. Thus, the said provision may not be the proper provision to hold Kho liable under the RPC

As for Belo and company, or those who copied the videos and leaked the videos online, they may be held liable for giving away or even selling the videos. "Giving away" means the distribution of indecent videos to many people and not merely casual, or occasional act of giving such kind of material to a single recipient.[38]

The owners of the website, as well as the Internet Service Provider, may be held liable for exhibiting the same material on the internet.

In case the acts of the individuals involved do not fall squarely under the provision of Article 201, then they may be prosecuted under Article 200, or Grave Scandals. Under the said offense, for one to be held liable for *arresto*

---

[35] Luis Reyes, THE REVISED PENAL CODE 339 (2006).

[36] People v. Atencio, CA-G.R. nos. 11351-R to 11353-R, December 14, 1954.

[37] Reyes, *supra* note 34.

[38] People v. Licuden, C.A., 66 O.G. 3173.

mayor and public censure, the offender must perform act or acts which are highly scandalous as offending against decency and good customs, and these acts should be committed in a public place or within the public knowledge or view.

b. Defamation

The uploading of sex scandals on the Internet generally leads to the humiliation of the persons shown in these scandals. The "actors" of these scandals may deny it, use it to climb to fame, but generally the victims of sex scandals suffer dishonor in society as a result of the publication online of their photographs or videos doing acts that are not meant for the public to see. Thus, they may also file a case for libel under Article 355 of the RPC.

Libel is defined as a public and malicious imputation of a crime, or a vice or defect, real or imaginary, or any act, omission, condition, status or circumstance tending to cause the dishonor, discredit or contempt of a natural or juridical person, or to blacken the memory of one who is dead.[39] If it is committed by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, or any similar means, the offender shall suffer the penalty of *prision correccional* in its minimum and medium periods or a fine ranging from 200 to 6,000 pesos, or both, in addition to the civil action which may be brought by the offended party.[40]

The act of uploading online a photograph or a video may fall under the catch all provision "any similar means" under the above-mentioned provision. The publication through the Internet of a sex scandal necessarily involves an imputation that the persons in those materials are of loose morals or even promiscuous, traits which are looked down upon in a traditional society as ours. Once malice is proved to have moved the offender in uploading the taking the videos and uploading them online, the said offender may be made liable under Article 355. Malice is presumed in every defamatory imputation.[41]

---

[39] REV. PENAL CODE, art. 353.

[40] *Id.*, art. 355.

[41] *Id.*, art. 354.

Those, on the other hand, who record or keep photographs or videos of the offended parties featured in those materials, to use it to threaten the offended party or to offer to prevent the publication of the material for material consideration can be held liable of grave threats or light threats, punishable by *arrestor mayor* or worse.

For acts which are not included and punished under the previous articles mentioned, and which cast dishonor, discredit or contempt upon the offended party, these acts may be punished as slander by deed under Article 359 of the RPC. The offenders who committed these acts would suffer the penalty of *arrestor mayor* in its maximum period to *prision correccional* in its minimum period or a fine ranging from 200 to 1,000 pesos.

Any person who shall publish, exhibit, or cause the publication or exhibition of any defamation shall be held responsible for the acts mentioned above. Thus, in Halili's case, the persons who took the video or caused the video to be taken, caused the video to be published online, and even those who are hosting the site where the video is being exhibited, are all liable for libel provided the elements of the same would be proven.

2. Under the Anti-Violence Against Women and Their Children Act of 2004

As mentioned earlier, Halili filed a complaint for violation the Anti-Violence against Women and Children Act, or Republic Act No. 9262 (R.A. 9262), against Kho. The said law seeks to value the dignity of women and children and guarantee full respect for human rights.[42]

Specifically, Halili filed a complaint for violation of Section 5 of the said act for psychological violence. Psychological violence under the said law refers to acts or omissions causing or likely to cause mental or emotional suffering of the victim such as, but not limited to, intimidation, *harassment,* stalking, damage to property, *public ridicule or humiliation*, repeated verbal abuse and mental infidelity.[43] If the offender engaged in purposeful, knowing, or reckless conduct, personally or through another, that alarms or causes substantial emotional or psychological distress to the victim, by engaging in any

---

[42] Rep. Act. No. 9262, §2 (2004). This is the Anti-Violence Against Women and Their Children Act of 2004.

[43] §3(a)(C).

form of violence or harassment,[44] or by causing mental or emotional anguish, public ridicule or humiliation to the victim,[45] then he would be liable under RA 9262.

For a woman to be able to file a complaint under the said law, it is required that she and the offender had a sexual or dating relationship.[46] A "*dating relationship*" refers to a situation wherein the parties live as husband and wife without the benefit of marriage or are romantically involved over time and on a continuing basis during the course of the relationship. A casual acquaintance or ordinary socialization between two individuals in a business or social context is not a dating relationship.[47] "*Sexual relations,*" on the other hand, refers to a single sexual act which may or may not result in the bearing of a common child.[48] Thus, a victim of a sex scandal may only file a case under this law if the person who made the scandal is or was engaged in a dating or sexual relationship with him or her. In Halili's case, she and Kho admitted to have had an affair, thus, they had a dating relationship. Moreover, as shown in the video, they did have sexual relations. Thus, Halili may file a case under this law. A complaint under RA 9262 however cannot be filed against those whom the victim had no relation with, such as the host of the website where the photograph or video was uploaded and the internet service provider.

Further, for victims who were forced to do indecent acts including being forced to "star" in the sex scandals, they can also file a complaint under RA 9262 for sexual violence.[49]

3. Under the E-Commerce Act

The E-commerce Act, or Republic Act No. 8792 (RA 8792) was passed as a reaction by the legislators to the criticism our country took for lack of computer laws in our country when the "love bug" was discovered to have originated from the Philippines.[50] RA 8792 is the first law in the country to explicitly penalize popular forms of cybercrimes.

---

[44] §5(h)((5).
[45] §5(i).
[46] §3(a).
[47] §3(e).
[48] §3(f).
[49] §3(a)(B).
[50] Disini, Jr. & Toral,, *supra* note 30.

In the Halili-Kho Sex Scandal, Belo and company were described to have accessed Kho's computer, without the latter's permission, and were able to view and copy the videos containing Kho's trysts with other women. Under RA 8792, the said acts may constitute hacking through unauthorized access punishable under the said law.[51] *Hacking* may be in any of the following forms: (1) unauthorized access into the computer; (2) interference in a computer system/server or information and communication system; (3) authorized access in order to corrupt, alter, steal, or destroy without the knowledge and consent of the owner of the computer or information and communications system; and, (4) the introduction of computer viruses and the like, resulting in the corruption, destruction, alteration, theft or loss of electronic data messages or electronic document. All types of unauthorized access are considered as hacking.[52]

a. Liabilities of the service providers

Once a sex scandal is posted online, many different entities including hosts, network providers, and access providers, would be involved. As they will often have deeper pockets than the author, the extent of their liability for hosting a defamatory content is of great significance.[53]

A service provider refers to the provider of online services or network access, or the operator of facilities therefore, including entities offering the transmission, routing, or providing of connections for online communications, digital or otherwise, between or among points specified by a user, of electronic data message or electronic documents of the user's choosing. It may also refer to the necessary technical means by which electronic data message or electronic documents of an originator may be stored and made accessible to a designated or undesignated third party. Such service providers shall have no authority to modify or alter the content of the electronic data message or electronic document received or to make any entry therein on behalf of the originator, addressee or any third party unless specifically authorized to do so, and shall retain the electronic data message or electronic document in accordance with the specific request or as necessary for the purpose of performing the services it was engaged to perform.[54]

---

[51] *See supra* note 28, §48.

[52] Disini, Jr. & Toral,, *supra* note 30.

[53] Graham Smith, INTERNET LAW AND REGULATION 171(2002).

[54] *See supra* note 28, §6(n).

Service providers would include Internet service providers (ISPs), application service providers, web hosting companies, domain name registries and registrars, online exchanges, websites hosting discussion groups and perhaps, any conceivable web-based online service company. In the case of SMS texting or even voice messaging, a cellphone company may be considered a service provider. The same is true for telephone companies in relation to their transmission of electronic data messages such as faxes or voice messages.[55]

Service providers may be made liable if they published, distributed or disseminated any electronic data message or electronic document which are unlawful. This would include defamatory content posted on the internet, such as sex scandals. The service provider would be liable under RA 8792 if was made aware of the defamatory content but did not advise the affected parties to refer to the appropriate authority or to alternative modes of dispute resolution; if it does not knowingly receive a financial benefit directly attributable to the defamatory content; and if the service provider does not directly commit any other unlawful act and does not induce or cause another person or party to commit other unlawful act and/or does not benefit financially from the unlawful act of another person or party.[56]

The liability of service providers under RA 8792 was based on American jurisprudence and required proof of editorial control by the service providers over the content to make them liable for defamation.[57] If the service provider lacked editorial control over the content located within its servers, as when it was a mere distributor of information, it would be absolved from liability for defamation.[58]

Note, however, that the service providers are not punished for hosting and publishing defamatory content such as sex scandals in itself. It is liable for failure to refer the parties to the appropriate forum to litigate or arbitrate their dispute. This is unlike the case of the liability of service providers under the Defamation Act of 1996 in United Kingdom, wherein the mere notice of a defamatory material being published by a service provider, and the failure to

---

[55] Disini, Jr. & Toral,, *supra* note 30.

[56] *See supra* note 28, §44.

[57] Disini, Jr. & Toral,, *supra* note 30.

[58] *See* Cubby, Inc. v. CompuServe, Inc., 776 F. Supp. 135 (S.D.N.Y. 1991).

remove the content after such notice, would make the service provider liable for defamation.[59]

4. The Anti-Child Pornography Law of 2009

This law was enacted late November 2009, and is not applicable in Halili's case. However, this is relevant for child victims of sex scandals.

For Republic Act No. 9775 (RA 9775), or the Anti-Child Pornography Law of 2009, to apply, the victim must be a child. The law defines a *child* to refer to a person below eighteen (18) years of age, or above 18 but is unable to fully take care of himself/herself from abuse, neglect, cruelty, exploitation or discrimination because of a physical or mental disability or condition. The term also refers to a person regardless of age who is presented, depicted or portrayed as a child, and to computer-generated, digitally or manually crafted images or graphics of a person who is represented or who is made to appear to be a child.[60]

This is the first major law aimed at protecting children from sexual exploitation through the making and distribution of the images of their abuse.[61] It seeks to protect every child from all forms of exploitation and abuse including the use of a child in pornographic performances and materials and the inducement or coercion of a child to engage or be involved in pornography through whatever means.[62]

This is also the first law to impose upon ISPs an active role in the prosecution of offenders in child pornography. An *ISP* under this law refers to a person or entity that supplies or proposes to supply, an internet carriage service to the public.[63] Under the law, they are bound to notify the Philippine National Police or the National Bureau of Investigation that any form of child pornography is being committed using its server or facility. They are also bound to preserve evidence for purposes of investigation. All ISPs are required to install available technology, program or software to ensure that access to or

---

[59] *See* Godfrey v. Demon Internet Ltd., 4 All E.R. 342. (1999).

[60] Rep. Act. No. 9775, §3(a) (2009). This is the Anti-Child Pornography Law of 2009.

[61] Shay Cullen, Anti-Child Porn Law Signed, The Mindanao Examiner, November 20, 2009, at http://www.mindanaoexaminer.com/news.php?news_id=20091120061145 (last visited Feb. 25, 2011).

[62] *See supra* note 60, §2(a).

[63] R.A. 9775, §3(g).

transmittal of any form of child pornography will be blocked or filtered.[64] Failure to comply with these tasks would hold the ISP liable for fines worth up to P2M and even revocation of their license.[65]

D. Anti-Voyeurism Law of the Philippines: Is this the Answer?

As shown above, there are existing laws in the Philippines under which the offenses that constitute sex scandals may be prosecuted. However, these laws were too general and were enacted not to specifically address and punish the offenses involved in sex scandals. They were merely made basis of possible complaints against offenders in sex scandals for lack of a specific law which punishes it. The only law previously discussed which does so is the Anti-Child Pornography Law of 2009, which, however, is limited only to cases wherein the victim is, or is depicted as, a child.

This does not mean, however, that the Philippine legislature is lacking in effort to enact a law to address the problem. The first Anti-voyeurism bill was filed by Miriam Defensor-Santiago in July 2007. But as a result of the Halili-Kho sex scandal, the Philippine Congress enacted Republic Act No. 9995, otherwise known as the Anti-Photo and Video Voyeurism Act of 2009.

The Act seeks to punish photo or video voyeurism. The law defines *Photo or video voyeurism* as the act of taking photo or video coverage of a person or group of persons performing sexual act or any similar activity or of capturing an image of the private area of a person or persons without the latter's consent, under circumstances in which such person or persons have a reasonable expectation of privacy. It also includes the act of selling, copying, reproducing, broadcasting, sharing, showing or exhibiting the photo or video coverage or recordings of such sexual act or similar activity through VCD, DVD, internet, cellular phones and similar means or device without the written consent of the persons involved, notwithstanding that consent to record or take photo or video coverage of same was given by such person.[66] The penalty of imprisonment of not less than three (3) years but not more than seven (7) years and a fine of not less than One hundred thousand pesos (P100,000.00) but not more than Five hundred thousand pesos (P500,000.00), or both, at the

---

[64] §9.

[65] §15(k).

[66] Rep. Act No. 9995, §3(d). *See also* §4 of the said law for a specific enumeration of the acts prohibited under the law.

discretion of the court shall be imposed upon any person found guilty of committing the offenses prohibited by the said law.

RA 9995 made punishable each offense that contributes to a sex scandal. The law prohibits the taking of photographs and videos of persons or a group of persons performing sexual activity or the like, under circumstances when the person or persons captured have a reasonable expectation of privacy, and when such taking is without the consent of the person or persons filmed[67]. *Reasonable expectation of privacy* is defined under this law as a situation wherein the offended party could disrobe in privacy, without being concerned that his or her image or private area was being captured. It could also refer to circumstances in which a reasonable person would believe that a private area of the person would not be visible to the public, regardless of whether that person is in a public or private place[68]. If the Halili-Kho sex scandal was taken when this law was already in effect and Halili made this as her basis for filing a case against Kho, if she could prove that she did not give her consent to Kho, contrary to what was found by the trial court in the dismissal of her case, the court may find Kho guilty for unauthorized taking of the video.

The law also punishes the act of copying and reproducing, or causing the copying or reproduction of the photo or video containing the sex scandal.[69] Again, in the context of the Halili-Kho Scandal, Belo, Chua and Rosario could be made liable under the said law for merely copying the sex scandal, even if they did not give copies to someone else so that the sex scandal would be uploaded on the internet. If Belo would argue that she did not copy the sex scandal, she could still be held liable for causing the copying of the sex scandal, as stated in her affidavit submitted before the National Bureau of Investigation wherein she said that she ordered Chua and Rosario to retrieve Kho's laptop to view and copy the videos.

Moreover, the DVD vendors are not spared. The law also punishes individuals who sell and distribute, or cause to be sold and distributed, such scandal[70]. If ever Belo, Chua or Rosario did sell the sex scandal to persons so that the said scandal could be sold and reproduced, they would also liable as the act punishes the selling of the original copy of the sex scandals.

---

[67] §4(a)
[68] §4(f)
[69] §4(b)
[70] §4(c).

Lastly, the law punishes individuals who publish or broadcast, or who cause to be published or broadcasted, the sex scandal.[71] *Broadcasting* means to make public, by any means, a visual image with the intent that it be viewed by a person or persons.[72]

The law gives complete protection to the victims of these sex scandals as broadcasting is broadly defined to prohibit the showing or exhibiting of the sex scandal through the Internet, cellular phones and any other similar means or device.[73] The service providers and even individuals who have copies of the sex scandal and who shows it to others would be made liable based on this prohibition.

These acts of copying, reproducing, selling, distributing and broadcasting are punishable even if the offended party gave his or her consent to the taking of the video.[74]

From the discussion, it can be said that before the Anti-Photo and Video Voyeurism Act, the laws under which offended parties in sex scandals can file their claim are too broad to specifically punish the acts which made possible the creation of a sex scandal. Victims would have to get parts and bits of laws just to have a cause of action against each and every person whose acts and degrees of participation in the making of the sex scandal differ. Further, the penalties imposed are not stiff enough to discourage offenders from repeating the same offenses. Moreover, the penalties imposed upon the perpetrators discourages a victim to come out and claim that he or she was wronged with the creation of a sex scandal, at the risk of being publicly ridiculed by society and be devoured by voyeurism that has prevailed in our old-fashioned society. Thus, sex scandals were not effectively prosecuted and offenders get off scot free.

Hopefully, with the enactment of the Anti-Photo and Video Voyeurism Act, the prevalence of sex scandals would go down and the dignity and privacy of the individuals involved would now be sufficiently protected. However, having a law as basis for prosecuting the offenders in sex scandals is

---

[71] §4(d).
[72] §3(b).
[73] §4(d).
[74] §4.

just the first step. The prosecution would still need to uncover evidence to prove the guilt of the accused beyond reasonable doubt.

As sex scandals easily proliferate with the aid of technology, the prosecution would need to be knowledgeable on the forms of evidence that they may use, the ways of discovering the said evidence, and the procedure for the presentation of these evidence before the court. These should all be done while still preserving the constitutional rights of the accused to privacy and against unreasonable searches and seizures. This, the author seeks to present in the following portion of the paper.

III. EVIDENCE IN THE DIGITAL AGE

A. Electronic Evidence: Making lives easier?

A desktop computer has a maximum capacity of up to 1.5 terabyte hard disk space[75], translating into hundreds of videos, music, pictures, computer programs, and documents. Just a small computer could store a room-full of things. In businesses, these could mean dozens of file-cabinets cramped into a small device. For students, it could mean hundreds of notes, reviewers, books, journal articles that he could bring along to class (if he has a laptop).

It is a fact of modern life that an enormous volume of information is created, exchanged, and stored electronically. Electronically stored information is commonplace in our personal lives and in the operation of businesses, public entities, and private organizations.[76]

It is so common that electronic data plays a substantial part in the proliferation of sex scandals. Kho kept the video of his sexual encounters in the hard drive of his laptop in electronic form. The same file was leaked through the Internet and could easily be opened and downloaded from the Internet by any person interested. Technological advances facilitated and made it easier to copy and transfer files – in the form of a video – than it was before.

---

[75] *Seagate Announced World's Largest Desktop Hard Drive Capacity at 1.5TB*, MY DIGITAL LIFE, *available at* http://www.mydigitallife.info/2008/07/12/seagate-announced-worlds-largest-desktop-hard-drive-capacity-at-15tb/ (last visited Nov. 28, 2010).

[76] Barbara J. Rothstein, Ronald J. Hedges, & Elizabeth C. Wiggins, *Managing Discovery of Electronic Information: A Pocket Guide for Judges*, FEDERAL JUDICIAL CENTER (2007).

1. What are electronic evidence?

Necessarily, the law enforcers and prosecutors involved in an investigation of sex scandals would necessarily have to encounter electronic evidence. *Electronic evidence*, as may be implied from the Rules on Electronic Evidence,[77] would include electronic data message and electronic documents in general.

An *electronic data message* refers to information generated, sent, received or stored by electronic, optical or similar means.[78] Generally, the term electronic data messages should be understood to mean any electronic file. It is *generated by electronic means* if it is created through electronic devices. This includes word processing and other computer files, electronic mail, SMS (short message service) messages, and other documents which are created through electronic devices. It is *sent or received by electronic means* if transmitted through telecommunications networks. It is *stored by electronic means* when the electronic data is not sent by the creator thereof but merely stored. It necessarily includes computer files which are not intended for transmission but mere storage.[79]

An *electronic document*, on the other hand, refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically. It includes digitally signed documents and any print-out or output, readable by sight or other means, which accurately reflects the electronic data message or electronic document. It may be used interchangeably with electronic data message.[80]

The videos and photographs of sex scandals, created by connecting the video camera recorder to the computer and saving the material as a file in the computer, are considered electronic data message or electronic document.

---

[77] A.M. No. 01-7-01-SC (2001).

[78] *See supra* note 29, Rule 2, §1; *See also supra* note 28, §6(e).

[79] Disini, Jr. & Toral,, *supra* note 30.

[80] *See supra note* 29,Rule 2, §1(h). *See also supra* note 28, §6(h) (2000).

Also of relevance are ephemeral electronic communication. An *ephemeral electronic communication* refers to telephone conversations, text messages, chatroom sessions, streaming audio, streaming video, and other electronic forms of communication the evidence of which is not recorded or retained.[81] In relation to sex scandals, these would include sex scandals of persons filmed and simultaneously streamed online, as mentioned earlier in the case of the New Jersey teenager who committed suicide.

2. The Problem: Physical Evidence vs. Electronic Evidence

The main problem of law enforcers investigating in sex scandals is how to obtain these types of files as evidence. But such task is not as easy as it sounds. Dealing with computer-related crimes in the Philippines is still in its infancy. The law enforcement agencies and the judicial system are still ill-equipped to handle high-tech cases, both in terms of experience and equipment.[82]

Moreover, electronic evidence is not the same as the traditional physical evidence recovered by crime scene investigators. The nature and distinct characteristics of electronic evidence, particularly it being electronically generated, stored and transferred, makes discovery and recovery of such evidence different than physical evidence.

The following items are just some characteristics of electronic evidence which poses problems to the prosecution's gathering of evidence.

a. Easy storage and transfer

First characteristic is that electronic evidence can be stored and transferred easily. If Kho lived in the 1980s where only Betamax and VHS tapes were used to store the videos, he would have a huge stack of tapes in his room which Belo could easily discover. If his friend Chua wanted to take revenge by distributing the tapes for everyone to see so that Kho and his girlfriend would be humiliated, he would have to spend hours making a copy of the whole tape. Thus, he would only be able to make a few copies – and

---

[81] *See supra note* 29, Rule 2, §1(k).

[82] AILYN CORTEZ, *Sex Scandals and Cyber Sex Informations* (2007), *available at* http://www.shvoong.com/law-and-politics/1683049-sex-scandals-cyber-sex-informations/ (last visited November 28, 2010).

only either in Betamax or in VHS tapes– in which case, he may opt to only make a single copy and just circulate it among a limited number of people.

Imagine it now in its digital form: the video, taken using a digital video recorder, would be uploaded to Kho's computer in a matter of seconds. It would be then stored in the computer's hard disk and he may place the videos in a folder named inconspicuously and innocently as "Fans file" or something. It would then be hard for other people, especially Belo, to know that he was keeping these video files.

Chua, on the other hand, after discovering that the "Fans file" folder in fact contained videos of Kho with women in compromising situations, decided to copy the said file. Since he wanted to make as many copies as possible, he uses optical disks like CDs, DVDs, or in USB flash drives. After copying the videos in a portable storage device as mentioned, he decides to copy the same to other data storage devices like his own computer, a laptop or palmtop, his MMS-enabled cellular phone and the like.[83]

And let us say, for example, that he is also the one who uploaded the video. The alleged website which first uploaded the videos of Kho alleged that their website merely receives through email videos from anonymous persons, and they in turn just upload the videos on their site.[84] How would the NBI agents, then, trace the video's source to be that of Chua's?

These examples merely show that with digital data, law enforcers would have to spend plenty of time, as well as patience, and should have the technical know-how in locating where the file is since it may be stored in several places, and it may be renamed and hidden so that its true contents would not be known. Issues on how digital evidence are obtained would be discussed in the latter part of this paper.

---

[83] *See generally* Cortez et al., *supra* note 31.

[84] Sandy Araneta & Reinir Padua, "3 persons in sex video upload case invited for questioning", Phil. Star, July 04, 2009, *available at* http://www.philstar.com/Article.aspx?articleid=483582 (last visited Feb. 22, 2011).

b. Easy alteration

Another trait of electronic evidence is that it could easily be altered using computer software. Take the case of Irish Sagud.[85] Her former boyfriend wanted to elope with her but she rejected his offer because he was about to get married to a girl he got pregnant. As his form of revenge, he superimposed her face on a picture of a naked woman with legs spread wide. He sent the said picture through Multimedia Message Service (MMS) and threatened Sagud that he could easily post it on the Internet. Fortunately, the Court convicted him of violation of R.A. 9262, even when the Court incorrectly remarked at that time that the Rules on Electronic Evidence does not apply to criminal actions.[86]

If this be applied in cases of sex videos, there are photo and video-editing softwares that could superimpose faces of people in videos. In case Halili denies that it was her in the video and treat it as acts that seek to tarnish her reputation, it would be possible to for her to file a criminal case for slander by deed or a civil case for damages.

Alteration of electronic evidence is not only a threatening situation for the law enforcers who are seeking evidence, it is also a dangerous trait of electronic evidence for the defense as the evidence may be easily altered to have the courts rule for his conviction. Problems on the integrity of the electronic evidence would be discussed later in the paper.

c. The Need for Technical Expertise

The last characteristic of electronic evidence, in relation to criminal prosecution, is that it's meaning and interpretation needs technical expertise. In the United States, the procedure adopted in most cases where digital evidence is involved is that the law enforcers would seize the computer of the accused, and would then submit the computer to an independent technical expert who would sort the files of the computer in accordance with the scope of the search warrant obtained by the law enforcers. This is allowed under the rule that the

---

[85] Rustan Ang vs. Court of Appeals, G.R. No. 182835 April 20, 2010.

[86] Initially, the Rules on Electronic Evidence were not made to apply to criminal action but the Court expanded its scope through A.M. No. 01-7-01-SC (RE: EXPANSION OF THE COVERAGE OF THE RULES ON ELECTRONIC EVIDENCE) issued September 24, 2002.

search made by a private person is within the purview of their Fourth Amendment.[87] This practice, however, is not resorted to in the Philippines because there are not much persons who may expertly perform such task in the country, and if ever there are, their services, as well as the equipment and gadgets that may be used to perform such task are costly.

As was shown, electronic evidence has distinct characteristics that law enforcers would need to give attention to, as compared to physical evidence. Unlike physical evidence which they can just label and store in boxes and keep pending court proceedings, electronic evidence needs more caution and technical expertise for it to be truly useful in court.

The discovery and recovery alone of electronic evidence poses problems for law enforcers. Complications add up when the law enforcers are tasked to preserve the constitutional rights of the accused while conducting the discovery and recovery of the evidence from him. Are these constitutional rights of the offenders fully protected under our legal system?

B. Evidence Gathering: A Problem on Its Own

When a cybercrime is involved and electronic evidence is sought to be seized, law enforcers have different approaches to achieve their goal. Some law enforcers first resort to surveillance of their suspects, while some, like in cases where there is an offended party who has with him (or her) some evidence needed to show probable cause for a complaint to prosper, just get search warrants to seek additional evidence.

1. Surveillance and the Issue of Privacy

Police enforcers are now attempting to keep up with their technological-savvy suspects by tracking them with the technology available. The most easily accessible way by which police enforcers track down and observe suspects in cybercrimes such as sex scandals, is to observe them through the Internet.

---

[87] United States v. Jacobsen, 466 U.S. 109, 113 (1984).

a. Surveillance through unsecured websites

Law enforcement agencies are now utilizing the Internet to their advantage: they use social networking sites and other public websites to monitor and trap their suspects.

In the case of the Ivan Padilla Gang, police officers used social networking sites such as Facebook and Twitter to track down the whereabouts of the gang and their leader. This led to the shoot-out of the leader, Ivan Padilla, and the arrest of some of the gang members.[88]

Police officers, as shown in TV shows such as *XXX* and *Imbestigador*, pose as customers on online sites for pornography and cybersex to determine where the business operation of the perpetrators are located and who the perpetrators are.

Police investigators now utilize the Internet to their advantage. Technology may complicate the prosecution of criminal offenses, particularly those involving cybercrimes, but all is not in vain as it may also aid law enforcers in capturing the suspects.

b. Surveillance through Third Parties

A suspect's electronic communications, such as phone calls, text messages, and e-mails may be stored on his computer, cellular phone, or other electronic device. In cases of sex scandals, it would be necessary for the law enforcers to discover the source of the photographs or videos to determine who should be prosecuted for causing the publication of such materials on the Internet. The key in most cases will be recovering the computer used to launch the attack. The records kept by most operating systems can allow forensics experts to reconstruct with surprising detail who did what and when.[89]

In Halili's case, NBI agents were able to locate the owners of the website where the sex scandal was first posted. The owners of the website

---

[88] *Philippine police use Twitter, Facebook to nail gang*, *available at* http://news.ph.msn.com/regional/article.aspx?cp-documentid=4255989 (last visited Nov. 28, 2010).

[89] Orin S. Kerr, *Digital Evidence and the New Criminal Procedure*, 1 COLUMBIA LAW REVIEW 279 (2005), *available at* HTTP://WWW.JSTOR.ORG/STABLE/4099310 (last visited Nov. 28, 2010).

admitted to the NBI that they were maintaining the website, but claimed that the videos were only sent to them through e-mail, and they did not know the identities of the persons who sent them the videos.[90]

It would thus be necessary to discover who sent the videos to the website owners. However, it is apparent that the Philippines do not have the technological means yet to do so as the true perpetrators behind the uploading of the sex scandals online have not been discovered yet. The law enforcers were not yet able to find the person whose computer contains the videos leaked through the internet. It must be noted, however, that it is possible to find out the source of the electronic mail and other relevant information through the help of third parties.

Copies of certain electronic communications—such as text messages and e-mails—may be held by service providers during or after transmission of those communications. Internet users routinely store most if not all of their private information on remote servers, and all of that information are available to system administrators. System administrators can read private e-mail, look through stored files, and access account logs that record how individual subscribers used the network.[91]

In most cases, the biggest investigative lead comes in the form of an originating Internet Protocol (IP) address recorded by servers. An *Internet Protocol address* is the unique identification of the location of an end-user's computer which serves as a routing address for email and other data sent to that computer over the Internet from other end-users.[92] However, IP Addresses are not necessarily assigned to a computer indefinitely and can be dynamically allocated by an Internet Service Provider (ISP). When an ISP dynamically allocates IP Addresses, it assigns IP Addresses arbitrarily to users for certain periods of time. One user can have used hundreds of IP Addresses over the course of a month, making identification of a user by her IP Address difficult.[93]

Most websites also store cookies in every Internet user's hard disk, making it easier to track down users who access a certain Internet website. A

---

[90]Araneta & Padua, *supra* note 83.

[91] Kerr, *Supra* note 88, at

[92] *Id.*

[93]Tara McGraw Swaminatha, The Fourth Amendment Unplugged: Electronic Evidence Issues & Wireless Defenses, Yale Journal of Law & Technology (2004-2005).

cookie is a file sent by a web server to a browser and then sent back by the browser each time it accesses that server. It is a computer data storage program which enables a web site to record, using information on a visitor's hard drive, his or her on-line activities. Cookies are pieces of information generated by a web server and stored on the visitor's computer.[94] In cases where a website exhibiting sex scandals claim that they just received the materials from visitors of their site, the law enforcement officers could access the cookies sent by the website to the viewers of the site to determine the identity of the individuals who sent the videos.

It is thus necessary for the law enforcement officers to have access to the information held by service providers in order to effectively pinpoint the real offenders in sex scandals. What would be the legal basis for these investigators to compel the assistance of service providers in our country?

Under the E-Commerce Act, service providers are required to retain the electronic data message or electronic document in accordance with the specific request or as necessary for the purpose of performing the services it was engaged to perform.[95] However, the law does not provide how law enforcement agents could access the information stored by the service providers, and the period for which the service providers are required to store information.

Under the Anti-Child Pornography Law, however, service providers are given an active role in the prosecution of child abusers. Internet service providers are tasked to notify the Philippine National Police (PNP) or the National Bureau of Investigation (NBI) within seven (7) days from obtaining facts and circumstances that any form of child pornography is being committed using its server or facility. It shall preserve such evidence for purpose of investigation and prosecution by relevant authorities. It shall, upon the request of proper authorities, furnish the particulars of users who gained or attempted to gain access to an internet address which contains any form of child pornography. ISPs shall also install available technology, program or software to ensure that access to or transmittal of any form of child pornography will be blocked or filtered. These provisions, however, are subject

---

[94] MARCUS TURLE, Data Protection, in ELECTRONIC COMMERCE: LAW AND PRACTICE (Alistair Kelman ed.).

[95] *Supra* note 28, § 6(n).

to the implementation of rules and regulation by the National Telecommunications Commission.[96]

Internet content hosts, on the other hand, who host or who propose to host internet content in the Philippines,[97] have similar duties with ISPs, but with the addition that they should not host any form of child pornography and the failure to remove any form of child pornography within forty-eight (48) hours from receiving the notice that any form of child pornography is hitting its server shall be conclusive evidence of willful and intentional violation of the law.[98]

No such provision, however, was provided in the Anti-Photo and Video Voyeurism Act of 2009. Neither is any mention of gathering information from third parties in the Rules on Electronic Evidence.

In the United States, resort to third party sources, such as service providers, are governed by their federal or state statutes.[99] The investigators utilize subpoenas to compel service providers to disclose information stored on their servers.[100] This method may be adopted in our country.

Another way where law enforcement agencies obtain information of the commission of cybercrimes through third parties is through the initial search conducted by private technicians. This is the case when the offenders in the sex scandals, particularly those who recorded the videos or took the photos without the knowledge of the persons in it have their computers for repair. This, however, is not a violation of the constitutional protection to an individual's privacy because the Bill of Rights does not protect citizens from unreasonable searches and seizures made by private individuals.[101]

---

[96] *See supra* note 59, §9.

[97] *Id.*, §3(f).

[98] *See supra* note 59, §11.

[99] Jeffrey Welty, *Prosecution and Law Enforcement Access to Information About Electronic Communications*, UNIVERSITY OF NORTH CAROLINA SCHOOL OF GOVERNMENT (2009), *available at* HTTP://WWW.SOG.UNC.EDU/PUBS/ELECTRONICVERSIONS/PDFS/AOJB0905.PDF (last visited Nov. 28, 2010).

[100] Kerr, *supra* note 88..

[101] Waterous Drug Corporation v. NLRC, G.R. No. 113271, October 16, 1997.

However, no matter how the investigators were able to retrieve information on offenders in cybercrimes such as sex scandals, there is bound to be an issue on the constitutional right of the accused to privacy and the accused would definitely raise this argument in order to make any evidence used against him inadmissible before the court.

c. Decrease in the Reasonable Expectation of Privacy?

The 1987 Constitution provides that "the privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise, as prescribed by law. Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding."[102]

The right to privacy provision was introduced in our 1935 Constitution. It was introduced as a reaction to the 1928 case of *Olmstead vs. US* (277 U.S. 438) [103] In this case, the court ruled that the government agents who had tapped the defendant's private telephone line without physical trespass did not violate the defendant's right to privacy because the government agents did not enter his private residence or office.

This case however was overruled in *Katz vs. United States* (389 U.S.347) where the court expanded the fourth amendment to protect modern contingencies not within the purview of the old test. In this case, police officers attached a listening and recording device to the outside of the telephone booth in which the defendant placed calls. The court held in this case that the fourth amendment protects people, not places. It further said that because an individual has a reasonable expectation of privacy in a telephone booth, the police officers violated the defendant's fourth amendment right against unreasonable searches and seizures.

Zones of privacy are likewise recognized and protected in our laws.[104] The Civil Code provides that "[e]very person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons" and punishes as actionable torts several acts by a person of meddling and

---

[102] Const. art. III, §3(1).

[103] JOAQUIN BERNAS, THE 1987 CONSTITUTION OF THE PHILIPPINES: A COMMENTARY (2003)

[104] *See* Blas Ople v. Ruben Torres Et al. G.R. No. 127685 July 23, 1998 293 SCRA 141 (1998).

prying into the privacy of another.[105] It also holds a public officer or employee or any private individual liable for damages for any violation of the rights and liberties of another person,[106] and recognizes the privacy of letters and other private communications.[107] The Revised Penal Code makes a crime the violation of secrets by an officer,[108] the revelation of trade and industrial secrets,[109] and trespass to dwelling.[110] Invasion of privacy is an offense in special laws like the Anti-Wiretapping Law,[111] the Secrecy of Bank Deposits Act[112] and the Intellectual Property Code.[113] The Rules of Court on privileged communication likewise recognize the privacy of certain information.[114]

As mentioned in the *Katz* case, whenever a person has a reasonable expectation of privacy, his right to it should be protected by the Constitution. The reasonableness of a person's expectation of privacy depends on a two-part test: (1) whether by his conduct, the individual has exhibited an expectation of privacy; and (2) whether this expectation is one that society recognizes as reasonable.[115]

---

[105] Article 26 of the Civil Code provides:

"Art. 26. Every person shall respect the dignity, personality, privacy and peace of mind of his neighbors and other persons. The following and similar acts, though they may not constitute a criminal offense, shall produce a cause of action for damages, prevention and other relief:

(1) Prying into the privacy of another's residence;

(2) Meddling with or disturbing the private life or family relations of another;

(3) Intriguing to cause another to be alienated from his friends;

(4) Vexing or humiliating another on account of his religious beliefs, lowly station in life, place of birth, physical defect, or other personal condition."

[106] CIVIL CODE, art. 32

[107] CIVIL CODE, art. 723.

[108] REV. PEN. CODE, art. 229.

[109] REV. PEN. CODE, art. 290-292.

[110] REV. PEN. CODE, art. 280.

[111] R.A. 4200.

[112] R.A. 1405.

[113] R.A. 8293.

[114] RULES OF COURT, Rule 130, §24.

[115] Ople v. Torres, G.R. No. 127685, 293 SCRA 141 (1998), *citing* Rakas v. Illinois, 439 U.S. 128, 143-144 [1978]; see the decision and Justice Harlan's concurring opinion in Katz v. United States, 389 U.S. 347, 353, 361, 19 L. ed. 2d 576, 583, 587-589 [1967]; see also Southard, "Individual Privacy and Governmental Efficiency: Technology's Effect on the Government's Ability to Gather, Store, and Distribute Information" (Computer/Law Journal, vol. IX, pp. 359, 367, note 63 [1989]).

However, it is argued that as technology advances, the level of reasonably expected privacy decreases.[116] The measure of protection granted by the reasonable expectation diminishes as relevant technology becomes more widely accepted. As one author has observed, previously, one could take steps to ensure an expectation of privacy in a private place, e.g., locking of doors and closing of curtains. Because advances in surveillance technology have made these precautions meaningless, the expectation of the privacy they offer is no longer justifiable and reasonable.[117] The security of the computer data file depends not only on the physical inaccessibility of the file but also on the advances in hardware and software computer technology.

Thus, investigators may argue that one who posts information about himself on the Internet has no reasonable expectation of privacy since, using the Katz test, his conduct of posting information online negates any expectation of privacy, and second, the Internet is open for the public to see, thus, it would be improbable to expect privacy in accordance with the society's standards.

There is a strong argument for the existence of a reasonable expectation of privacy, however, when it comes to content of electronic documents and data messages.[118] Note that there are a few allowable exceptions to this rule, depending on whether the sender was an employee, whose employer warned him or her that messages sent from his or her work computer were subject to inspection; whether the sender's Internet service provider (ISP) provided for monitoring in its user agreement; and whether a third party received and reviewed the message before it was obtained by law enforcement officers.[119]

There is yet no jurisprudence in the Philippines to rule on the issue. It is suggested that the analysis should be based on whether a wire containing internet traffic should be deemed private or public space for determining

---

[116] Ople v. Torres, G.R. No. 127685, 293 SCRA 141 (1998), *citing* Dennis Southard, *Individual Privacy and Governmental Efficiency: Technology's Effect on the Government's Ability to Gather, Store, and Distribute Information*, COMPUTER/LAW JOURNAL, vol. IX, pp. 359, 369 (1989).

[117] Dennis Southard, *Individual Privacy and Governmental Efficiency: Technology's Effect on the Government's Ability to Gather, Store, and Distribute Information*, COMPUTER/LAW JOURNAL, vol. IX, pp. 359, 369 (1989).

[118] Welty, *supra* note 98.

[119] *Id.*

reasonable expectation of privacy. If courts view wires of internet traffic as public spaces in which individuals cannot retain a reasonable expectation of privacy, traditional rules will impose no constitutional limits on surveillance of law enforcers. If courts construe them as private spaces that do support a reasonable expectation of privacy, surveillance designed to target even non-private information will nonetheless require strong legal justification.[120] We would have to wait for the Philippine Supreme Court to have a definite ruling on the matter, but as the technology available to our law enforcement agencies are dismal and outdated, it may take years before such ruling would be made.

2. Searches and Seizure

The Constitution provides that the right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.[121] Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding.[122]

For government agents to be able to access information kept by service providers and by individuals to effectively prosecute cybercrimes such as sex scandals, it would need to procure a search warrant. The E-Commerce Act provides that access to an electronic file, or an electronic signature of an electronic data message or electronic document shall only be authorized and enforced in favor of the individual or entity having a legal right to the possession or the use of the plaintext, electronic signature or file and solely for the authorized purposes.[123]

Under the Rules of Court, a search warrant shall not issue except upon probable cause in connection with one specific offense to be determined personally by the judge after examination under oath or affirmation of the

---

[120] Kerr, *supra* note 88.

[121] *Supra* note 101, art. III, §2.

[122] *Id.*, art. III, §3(2).

[123] *See supra* note 28, §45 (2000).

complainant and the witnesses he may produce, and particularly describing the place to be searched and the things to be seized which may be anywhere in the Philippines.[124] Thus, for a valid search warrant to issue, the following requisites should be present: (1) It must be issued upon probable cause; (2) Such probable cause must be determined by the issuing magistrate personally; (3) the issuing magistrate must have personally examined, in the form of searching questions and answers, the applicant and his witnesses and taken down their written depositions; (4) the search warrant must particularly describe or identify the property to be seized as far as the circumstances will ordinarily allow; (5) It must particularly describe the place to be searched; (6) if shall issue for only one specific offense; and (7) It must not have been issued more than ten days prior to the search pursuant thereto.[125]

However, unlike searches in the physical realm, searches and seizure of data in the cybercrimes introduces issues with regard to the particularity of description in the search warrant and the application of the plain-view doctrine.

a. Particularity of Description of Search Warrants

The Constitution provides that no search warrant shall issue unless the search warrant particularly describe the "place to be searched and the persons or things to be seized."[126] Initially provided in response to Kings George II and George III's acts of allowing the search and ransacking of houses to obtain evidence by simply issuing a "general warrant, "[127] this requirement is primarily meant to enable the law enforcers serving the warrant to readily identify the properties to be seized and thus prevent them from seizing the wrong items; and leave said peace officers with no discretion regarding the articles to be seized and thus prevent unreasonable searches and seizures.[128]

A search warrant particularly describes the thing to be seized when a description therein is as specific as the circumstances will allow; when it expresses a conclusion of fact by which the warrant officer may be guided; or

---

[124] *See supra note* 113, Rule 126, §4.

[125] FLORENZ REGALADO, REMEDIAL LAW COMPENDIUM VOLUME TWO 643 (2004). (Citations omitted).

[126] *See supra* note 101, art. III, §2.

[127] *See supra* note 102.

[128] People vs. Tee, G.R. Nos. 140546-47, January 20, 2003; See also Corro v. Lising, 137 SCRA 541 and People v. Damaso, 212 SCRA 457.

when the things described are limited to those which bear a direct relation to the offense for which the warrant is issued.[129]

However, in the computer-based world, each person may have a desktop computer, plus disks or other removable data storage media, a laptop computer, a home computer, and a hand-held personal organizer, all potentially containing relevant data. Offsite and even offshore data storage facilities, Internet service providers, and other third parties may also hold data subject to discovery.[130] Further, files which contain evidence relevant to the prosecution of sex scandals may be hidden in a secret file folder, or labeled with an inconspicuous name that it would be impossible for investigators to describe with particular specificity the evidence (in the form of electronic evidence) they seek to seize.

What law enforcers would tend to do is to simply list the location of the physical search as the location where the warrant will be executed. For example, the police received a tip that a certain video or photograph circulating as a sex scandal was created and was uploaded by Person A living in House No. 1, Somewhere Street, Nowhere land. The police would just specify the said address in the search warrant, and would claim that the said address reasonably describes with particularity the location of the electronic evidence sought to be obtained. However, this is only the location of the physical search, not the electronic search.[131]

If law enforcers attempt to be specific, should the search be limited only to a particular folder or sub-directory? This, however, may not achieve the purpose for which the search warrant was applied as there would be no guaranty that the data sought to be recovered is in the said folder or subdirectory since electronic data may be easily moved, renamed or transferred.[132]

---

[129] REGALADO, *supra* note 124, at 644. (Citations omitted).

[130] Kenneth Withers, *Computer-based Discovery in Federal Civil Litigation*, FEDERAL COURTS REVIEW, *at* HTTP://WWW.FJC.GOV/PUBLIC/PDF.NSF/LOOKUP/ELECDI01.PDF/$FILE/ELECDI01.PDF (last visited Nov. 28, 2010), *citing* Michael R. Overly, *Electronic Evidence in California* (1999) 2-31.

[131] Oris S. Kerr, *Search Warrants in an Era of Digital Evidence*, 75 MISSISSIPPI L.J. 85 (2005).

[132] U.S. v. Hill, 459 F.3d 966, at 978.

As for items to be seized, our Rules of Court only allow the seizure of the subject of the offense, the fruits of the offense or the items used or intended to be used as the means of committing an offense.[133] If the computer is the instrumentality of the crime and falls under the third category, the search warrant can just describe the computer to be seized. But if the computer is just the storage of evidence for the evidence, and there is no certainty that the said computer was used as an instrument of the crime,[134] should the courts require that the search warrant be more specific as to what electronic evidence should be seized?

The Philippine Supreme Court has yet to squarely address this issue. The nearest it has come to facing the issue is in the case of *Microsoft Corporation vs. Maxicorp Inc.*[135] This case involved an alleged copyright infringement on the part of Maxicorp. Maxicorp allegedly produced pirated copies of Microsoft's softwares. Search warrants were obtained to enable law enforcers to raid and seize materials from Maxicorp's premises that would support the allegation. Maxicorp filed a motion to quash, saying that there was no probable cause and that the warrants of arrest were general warrants.

The court partially granted the petition filed by Maxicorp, saying that there was probable cause that supported the search warrants. The court however found that part of the search warrant lacked particularity because it authorized the seizure of not only those which were alleged to have been used in the copyright infringement of Microsoft's products, it may also have included property used for personal or other purposes not related to copyright infringement or unfair competition. Moreover, the description covered property that Maxicorp may have bought legitimately from Microsoft or its licensed distributors. The objects which were lawfully seized, however, are considered to have been used or intended to be used as the means of committing the crime and therefore no issue arises as to specificity in the search warrant as to electronic evidence.

To evade the issue, the Court would just refer to the principle that a search warrant should be specific only as far as the circumstances will ordinarily allow. In the words of the court, "the description of the property to be seized need not be technically accurate or precise. The law does not require

---

[133] *Supra* note 113, Rule 126, §3.

[134] Kerr, *supra* note 130.

[135] G.R. No. 140946. September 13, 2004.

that the things to be seized must be described in precise and minute details as to leave no room for doubt on the part of the searching authorities; otherwise it would be virtually impossible for the applicants to obtain a search warrant, as they would not know exactly what kind of things they are looking for. Once described, however, the articles subject of the search and seizure need not be so invariant as to require absolute concordance, in our view, between those seized and those described in the warrant. Substantial similarity of those articles described as a class or species would suffice. The nature of the description should vary according to whether the identity of the property or its character is a matter of concern."[136]

In the age of modern technology and commercial availability of various forms of items, the warrant could not be expected to describe with exactitude the precise form the records would take, and that the seizure of a specific item characteristic of a generic class of items (items that record information) defined in the warrant would not constitute an impermissible general search.[137]

b. How Seizure of Electronic Evidence is Conducted

b.1 Seizure of the Whole Computer

This is the most common way by which investigators obtain electronic evidence. This is generally allowed when the computer seized is used as the instrumentality of the crime.[138] The police investigators would unplug the computers from the crime scene and bring it to a laboratory to be examined by a trained digital evidence examiner. The examiner then makes a "forensically sound" copy of the computer's hard drive and reviews the copy for evidence or contraband. Upon completion, the examiner reports the findings back to the investigator.[139]

---

[136] Yao, Sr., et al. v. People, et al., G.R. No. 168306, June 19, 2007, 525 SCRA 10; Microsoft Corporation vs. Maxicorp. Inc., G.R. No. 140946, September 13, 2004, 438 SCRA 224.

[137] U.S. *v. Giberson.* (9th Cir. 2008) 527 F.3d 882.

[138] This is allowed under the Rules of Court, Rule 126, §3(c). *See also* U.S. v. Campos, 221 F.3d 1143 (10th Cir. 2000).

[139] Todd G. Shipley & Henry R. Reeve, *Collecting Evidence from a Running Computer: A Technical and Legal Primer for the Justice Community,* Legal Committee of the Working Group of the Internet Crimes Against Children Task Forces at www.search.org (last visited Nov. 28, 2010), *citing* U.S. Department of Justice, Office of Justice Programs, National Institute of Justice 1 (Washington, DC: April 2004).

Deleted data may even be recovered during the course of the examination, as a delete function normally just marks storage space as available for new material and does not actually erase anything.[140] Hitting the "delete" key merely renames the file in the computer, marking it available for overwriting if that particular space on the computer's hard disk is needed in the future. The data may remain on the hard disk or on removable storage media for months or years, or may be overwritten only partially.[141]

The primary reason for authorizing law enforcement to seize an instrumentality of crime is to prevent future crimes. When deciding whether or not a piece of hardware can be seized as an instrumentality of crime, it is important to remember that "significant" is the operative word in the definition of instrumentality. Unless a plausible argument can be made that *the hardware played a significant role in the crime*, it probably should not be seized as an instrumentality of the crime.[142]

Courts deem it reasonable for the whole computer to be seized based on what is coined "*The Container Theory*". According to this doctrine, a search warrant authorizing the seizure of materials also authorizes the search of objects that could contain those materials. Computers, like briefcases and cassette tapes, can be repositories for documents and records.[143]

This was based on the case of *United States v. Gomez-Soto,*[144] wherein officers were conducting a search pursuant to a warrant authorizing the seizure of "books, papers, records, receipts, documents, notations, diaries, journals or ledgers" related to the defendant's unlawful business dealings. During the search, the officers found a locked briefcase and a microcassette tape. After the defendant refused to open the briefcase, the officers cut it open and seized its contents, which included cocaine. The microcassette tape contained incriminating statements about the defendant.

The defendant challenged the search, arguing that the search and seizure of the briefcase, the microcassette, and their contents were not

---

[140] United States v. Upham, 168 F.3d 532, 533 (1st Cir. 1999)

[141] Withers, *supra* note 129, *citing* Andy Johnson-Laird, Smoking Guns and Spinning Disks, 11 COMPUTER LAW. 1 (1994).

[142] Casey, *supra* note 20, 36.

[143] *See supra* note 136.

[144] 723 F.2d 649, 652 (9th Cir.1984).

permitted because they were not particularly described in the warrant. The court held that the search and seizure of both the microcassette and the briefcase were proper. It is axiomatic that if a warrant sufficiently describes the premises to be searched, this will justify a search of the personal effects therein belonging to the person occupying the premises if those effects might contain the items described in the warrant. Because the briefcase would be a logical container for many of the items described in the warrant, and the microcassette tape is, *by its very nature a device for recording information which comes clearly within the specific authority of the warrant*, the court held that the failure of the warrant to anticipate the precise container in which the material sought might be found was not fatal.

However, the seizure of the computer might expose the owner of the computer to the danger that privileged communication, especially evidence that are not be covered by the search warrant, would be discovered by the law enforcers. Because computers can hold so much information touching on many different areas of a person's life, there is a greater potential for the 'intermingling' of documents and a consequent invasion of privacy when police execute a search warrant for evidence on a computer.[145]

This is a common situation in the United States when law enforcers obtain a search warrant for a specific crime involving the computer, and then seize the computer, but later on finds child pornography, possession of which are punishable under their federal and state laws. However, courts upheld conviction of the offenders in those cases under the "plain-view" doctrine.[146]

Although the 'intermingling' of documents may be a valid defense, as the constitutional right to privacy of the accused is also at stake, the Courts generally upheld the validity of the search as to the documents seized pursuant to the search warrant. The fear that agents searching a computer may come across personal information cannot alone serve as the basis for excluding evidence of criminal acts.[147] While officers ought to exercise caution when executing the search of a computer, just as they ought to when sifting through documents that may contain personal information, the potential intermingling of materials does not justify an exception or heightened procedural protections

---

[145] *See supra* note 136, *citing* United States v. Walser, 275 F.3d 981, 986 (10th Cir.2001).

[146] See U.S. V. CAREY, 172 F.3D 1268 (10TH CIR. 1999); U.S. v. Gray, 78 F. Supp. 2d 524 (E.D. Va. 1999); and U.S. v. Wong, 334 F.3d 831 (9th Cir. 2003).

[147] U.S. v. Adjani, 452 F.3d 1140, at 1152.

for computers beyond the constitutional right to privacy's reasonableness requirement.[148] No provision of law exists which requires that a warrant, partially defective in specifying some items sought to be seized yet particular with respect to the other items, should be nullified as a whole. A partially defective warrant remains valid as to the items specifically described in the warrant.[149]

It is certain that over-seizing of data as an inherent part of the electronic search process would be more common now than in the days of paper records. Note, however, that the US Court in *US v. Comprehensive Drug Testing, Inc.*[150] called for greater vigilance on the part of judicial officers in striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures. It believed that the process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect. This, however, is not yet the prominent view in recent American jurisprudence.

b.2. Copying files from the Computer

It is common for digital investigators to read data from pagers, mobile phones, and personal digital assistants directly from the devices. Copying of files, as opposed to seizure of the computer itself, is deemed to be a "less intrusive search method" in relation to the right of the accused against unreasonable searches and seizure.[151] However, this approach does not provide access to deleted data and may not be possible if the device is password protected or does not have a way to display the data it contains.[152]

There are specialized tools developed to achieve a complete and thorough search of the computer and to enable the investigators to obtain all the relevant data needed. Tools have been developed to access password protected and deleted data (ZERT, TULP, and Cards4Labs). More sophisticated techniques involving electron microscopes are also available to recover encrypted data from embedded systems. The problem is that these

---

[148] *See supra* note 136.

[149] Microsoft Corporation vs. Maxicorp. Inc., G.R. No. 140946, September 13, 2004, *citing* People v. Salanguit, G.R. Nos. 133254-55, 19 April 2001.

[150] 513 F.3d 1085 (9th Cir. 2008).

[151] U.S. v. Gawrysiak, 972 F. Supp. 853, aff'd, 178 F.3d 1281 (3d Cir. 1999).

[152] Casey, *supra* note 20,28.

technological advancements are prohibitively expensive for most purposes and many individuals are still unaware of it.[153]

Courts have usually been lenient in how evidence are recovered from computers. But hopefully with the increase in technical know-how of judges and justices, courts would come up with rulings such as in *Gates Rubber Co. v. Bando Chemical Indus. Ltd.*[154] Here, the investigator merely copied individual files from the computer. The court criticized the investigator for not using "the method which would yield the most complete and accurate results", when specialized digital evidence processing tools are available to them.

b.3. Conducting a "Running Search"[155]

A *running computer* is defined as a computer that is already "powered on" when encountered at a crime scene. It is important to note that potential evidence may be lost or destroyed if a running computer is encountered by law enforcement and seized as part of an investigation using the accustomed methodology described above. This search method was developed to address the advancement of the home networking technology, wherein small wired or wireless networks are setup in one's own home to connect different devices into a single pool of information.

Volatile data on running computers can provide crucial evidence. Computers require that a certain amount of computer memory called *random access memory* (RAM) be used by the operating system and its applications when the computer is in operation. The computer utilizes this RAM to write the current processes it is using as a form of a virtual clipboard. The information is there for immediate reference and use by the process. This type of data is called *volatile data* because it simply goes away and is irretrievable when the computer is off. Volatile data stored in the RAM can contain information of interest to the investigator. Examples that may be considered relevant for cybercrime prosecutors are the identity of the person who is logged into the system; the open ports and listening applications; the lists of currently running processes; the registry information; the system information; and the attached

---

[153] *Id.*

[154] 9 F.3d 823 (10th Cir. 1993).

[155] *Discussion taken from supra* note 129.

devices which can be important if there is a wireless-attached device not obvious at the crime scene.

3. The Issue of Plain View Doctrine in Gathering Electronic Evidence

Objects in the "plain view" of an officer who has the right to be in the position to have that view are subject to seizure and may be presented as evidence. The plain view doctrine is usually applied where the police officer is not searching for evidence against the accused, but nonetheless inadvertedly comes upon an incriminating object.[156]

For a search and seizure to be valid under the plain view doctrine, there must be the concurrence of the following requisites: (a) a prior valid intrusion based on the valid warrantless arrest in which the police are legally present in the pursuit of their official duties; (b) the evidence was inadvertedly discovered by the police who have the right to be where they are; (c) the evidence must be immediately apparent; and (d) "plain view" justified the seizure of the evidence without any further search.[157]

An object is in plain view if the object itself is plainly exposed to sight. If the package or if its contents, whether by distinctive configuration, its transparency, or if its contents are obvious to an observer, then the contents are in plain view and may be seized.[158]

Applying the doctrine to searches and seizure of computers in relation to the prosecution of cybercrimes, when a police officer obtains a search warrant for the computer to obtain electronic evidence in sex scandals, and in the course of inspection he finds electronic evidence that could implicate the possessor of the computer to other crimes like software piracy, the discovery of evidence implicating the possessor of the computer for the latter crime may be justified under the doctrine of "plain view". This may especially be the case

---

[156] People v. Musa, 217 SCRA 597.

[157] ANTONIO NACHURA, OUTLINE/REVIEWER IN POLITICAL LAW132 (2006), *citing* People v. Musa, *supra*; People v. Aruta, G.R. No. 120515, April 13, 1998; People v. Doria, G.R. NO. 125299, January 22, 1999; and People v. Sarap, G.R. No. 132165.

[158] Caballes v. CA, G.R. No. 136292, January 15, 2002.

when the crime for which the warrant was obtained requires technical expertise from the possessor of the computer, such as computer hacking.[159]

The doctrine, however, may be subject to abuse of law enforcement agents. This possibility was recognized in the case of *United States v. Comprehensive Drug Testing, Inc.*,[160] wherein the en banc court found that applying the doctrine to digital searches and seizures creates potential for abuse: Officers could seize massive quantities of data on the premise that it includes at least some evidence that is within the scope of their warrant; then, as they go through the data, they can seize (and use) (i) evidence that is within the scope of the warrant and (ii) evidence that is not within the scope of the warrant but that is seizable under the plain view doctrine. The en banc court found that to prevent abuse, magistrates who issue digital search warrants must require the government to "forswear reliance on the plain view doctrine or any similar doctrine that would allow it to retain data to which it has gained access only because it was required to segregate seizable from non-seizable data". This ruling might mitigate the risks when the computers are, as a whole, seized from the suspected offenders.

4. Resort to Modes of Discovery

The more popularly known modes of discovery depositions, interrogatories and request for admissions – are commonly resorted to in civil cases. Philippine jurisprudence touching on the topic provides that the rationale behind the recognition accorded the modes of discovery is that they enable a party to discover the evidence of the adverse party and thus facilitate an amicable settlement or expedite the trial of the case.[161]

Courts are tasked to encourage the use of different modes of discovery, and it is indeed "the duty of each contending party to lay before the court all the material and relevant facts known to him, suppressing or concealing nothing, nor preventing another party, by clever and adroit manipulation of the technical rules of evidence, from also presenting all the facts within his knowledge."[162] Thus, in discovery proceedings, one cannot

---

[159] U.S. v. Gray, 78 F. Supp. 2d 524 (E.D. Va. 1999).

[160] U.S. v. Comprehensive Drug Testing, Inc., 513 F.3d 1085 (9th Cir. 2008)

[161] Ong v. Mazo et al. ,G.R. No. 145542, June 04, 2004.

[162] FLORENZ REGALADO, REMEDIAL LAW COMPEDIUM 305-306 (Sixth Revised Edition), *citing* Koh v.IAC, G.R. No. 71388, September 23, 1986..

strongly invoke his rights against self-incrimination as this would be deemed suppression of evidence.[163]

It is a fallacy, however, to state that there are no available modes of discovery in criminal prosecution. The various modes of discovery enumerated and provided for in the Rules of Civil Procedure are expressly made applicable to criminal proceedings.[164] The accused can subpoena witnesses and documents held by the prosecution.[165] The accused may also move for bill of particulars before arraignment to enable him properly to plead and prepare for trial.[166] The accused may also move for the production and permission of the inspection and copying or photographing of any written statement given by the complainant and other witnesses in any investigation of the offense conducted by the prosecution or other investigating officers, as well as any designated documents, papers, books, accounts, letters, photographs, object, or tangible things not otherwise privileged, which constitute or contain evidence material to any matter involved in the case and which are in the possession or under the control of the prosecution, police, or other law investigating agencies. This may be granted by the court upon showing good cause, and in order to prevent surprise, suppression, or alteration of evidence.[167]

The prosecution, however, is not generally allowed to go on a "fishing expedition" to prove the guilt of the accused. The burden of proof is on the party who asserts an affirmative allegation.[168] If guilt of the accused is not shown by proof of guilt beyond reasonable doubt, or that degree of proof which produces conviction in an unprejudiced mind, then the accused is entitled to an acquittal.[169]

C. Presentation of Electronic Evidence

The Rules on Electronic Evidence was made effective on 1 August 2001 and initially applied to civil, quasi-judicial and administrative proceedings pending after the date of effectivity, and was a direct result of the enactment of Republic Act No. 8792, or the Electronic Commerce Act. The Rules were

---

[163] *See* Qualcomm Inc. v. Broadcom Corp., 2008 WL 66932 (S.D. Cal. Jan. 7, 2008).
[164] Republic vs. Sandiganbayan G.R. No. 90478 November 21, 1991
[165] *See supra* note 113, Rule 21 (1997).
[166] *Id.*, Rule 116, §9.
[167] *See supra* note 113, Rule 116, §10.
[168] *Id.*, Rule 131, §1.
[169] *Id.*, Rule 133, §2.

amended on 24 September 2002 to include criminal cases in its coverage, effective 24 October 2002, pursuant to A.M. No. 01-7-01-SC (Re: Expansion of the Coverage of the Rules on Electronic Evidence).

The said rules, along with the E-Commerce Act, paved way for the admissibility of electronic evidence, as presented before the courts. Information should not be denied validity or enforceability solely on the ground that it is in the form of an electronic data message or electronic document, purporting to give rise to such legal effect. Electronic data messages or electronic documents shall have the legal effect, validity or enforceability as any other document or legal writing.[170]

The paper presented earlier how sex scandals as cybercrimes may be punished under our laws. The paper also showed how evidence may be obtained in order to prosecute these offenses. The only problem left is how to present these pieced of evidence before the court, and how to determine the integrity of the evidence offered as evidence.

1. Form of evidence offered for presentation

Since electronic documents would be necessarily stored in computers, the issue of whether presenting printouts of the documents is enough has been debated. Many computer-based documents, such as relational databases and spreadsheets, are meaningless in printed form.[171] The form may have important implications on how easily, if at all, the information can be electronically searched, on whether relevant information is obscured or sensitive information is revealed, and on how the information can be used in later stages of the litigation.[172]

The Philippine Supreme Court has not made a definite ruling on how electronic evidence should be presented before the courts. In *Libayhay v. Canda,*[173] an administrative case involving a clerk of court and a Municipal Circuit Trial Court judge, text messages were presented before the court to prove threats and indecent messages through text allegedly sent by the MCTC judge. There is no discussion, however, on how it was presented in the

---

[170] *See supra* note 29, Rule 3; *See also supra* note 28, § 7 (2000).

[171] *See supra* note 129.

[172] Rothstein, Hedges & Wiggins, *supra* note 75.

[173] A.M. No. MTJ-06-1659. June 18, 2009.

proceedings.[174] Text messages were held to be admissible as ephemeral electronic communication.

2. Integrity of Electronic Documents: The Danger of Alteration

The adversarial system of litigation causes problems because it will always be in the interests of one side to suggest that unreliable evidence is reliable and vice versa. Without independent inquisitorial resources to determine reliability, the court has a task which it rarely addresses.[175]

Integrity of the electronic evidence would always be made an issue because of the ease of altering the contents of electronic evidence. But the integrity of an electronic may be maintained. This is established by showing that "(it) has remained complete and unaltered, apart from the addition of any endorsement and any authorized change, or any change which arises in the normal course of communication, storage and display."[176] Hence, the addition of message headers, digital signatures, and other marks to the electronic document will not detract from its status as "writing."[177]

The integrity of an electronic evidence may be established by showing any of the following: (a) By evidence that at all material times the information and communication system or other similar device was operating in a manner that did not affect the integrity of the electronic document or electronic data message, and there are no other reasonable grounds to doubt the integrity of the information and communication system; (b) By showing that the electronic document or electronic data message was recorded or stored by a party to the proceedings who is adverse in interest to the party using it; or, (3) By showing that the electronic document or electronic data message was recorded or stored in the usual and ordinary course of business by a person who is not a party to the proceedings and who did not act under the control of the party using the record.[178]

---

[174] *See also* Nuez v. Cruz-Apao, A.M. No. CA-05-18-P, April 12, 2005; Ang v. CA, G.R. No. 182835, April 20, 2010; Vidallon-Magtolis v. Salud, A.M. No. CA-05-20-P, September 9, 2005.

[175] Alistair Kelman, *Evidence and Security*, ELECTRONIC COMMERCE: LAW AND PRACTICE, at 197 (3rd ed.).

[176] Section 10[b][i], IRR of the E-Commerce Act.

[177] Disini, Jr. & Toral,, *supra* note 30.

[178] *See supra* note 28, § 17. *See also supra* note 29, Rule 5.

The trustworthiness of content and the process of recording and storing it form the actual reliability of the evidence. Factors which have to be taken into account in determining the trustworthiness can include the quality of the original source, the quality of the internal computer manipulations, the strength of any control or audit mechanism which might reduce error or provide corroboration, the integrity of the way in which an exhibit – what the court actually considers s- has been derived, and integrity of the way in which the exhibit has been handled by or brought into being by investigators.[179]

IV. ARE WE READY? AN ASSESSMENT OF THE STATE OF THE PHILIPPINE LEGAL SYSTEM IN THE PROSECUTION OF SEX SCANDALS

As shown in the first part of the paper, there are laws of general character which were used to file complaints against offenders in sex scandals. The penalty for these crimes would vary, but in general, the penalties for the said crimes are trivial and would not deter offenders from repeating it.

The passage of the Anti-Voyeurism Law in the Philippines provided a comprehensive law which would make punishable acts involved in the commission of sex scandals. The law, however, does not impose an active duty upon the service providers to participate in the investigation and retention of evidence that may be used to prosecute the offenders. The Anti-Child Pornography Law has fared better on this aspect, imposing upon Internet Service Providers and Content hosts positive duties to help mitigate the incident of sex scandals as to children.

The second part of the paper presented the issues faced by law enforcement agents in recovering evidence that may be used to prosecute sex scandal offenders. There is, however, lack of specific rules, or if there are rules, lack of implementing rules to facilitate the collection of electronic evidence and at the same time, to safeguard the right of the accused against unreasonable searches and seizure and his right to privacy.

The third part of the paper raises the possible issues that would be faced by the parties in the prosecution of sex scandals when they are already before the court. The Supreme Court has not made a definite ruling, nor provided specific guidelines on the proper procedure for offering electronic

---

[179] Kelman, *supra* note 174, at 199.

evidence before courts. This may indicate the acceptance of the courts to electronic evidence as a form of evidence, or the lack of technical knowledge of the courts to recognize issues and problems in presenting the same.

Overall, the author is of the opinion that the Philippines is on the right track. As opposed to the situation back in 2000 where the country was criticized all over the world for not being able to prosecute the person who created the "love bug" for lack of applicable laws, the country today has the right mechanisms and legal framework to facilitate the faster integration of electronic evidence in judicial proceedings.

However, there should be an increased awareness and knowledge on the part of the legislature and the judiciary as to the intricacies and dilemmas in the effects of technological advances on criminal prosecution. When the judiciary and the legislature are now aware of the issues involved and their underpinnings, they could then take on the subject with zeal instead of brushing it aside.

Further, the legislature and the judiciary should formulate new rules and laws which specifically address the issues posed by the emergence of cybercrimes and electronic documents. The Cybercrime Bill has been pending before the congress for quite some time now and has not yet been enacted. There are no rules yet regulating searches and seizures when dealing with electronic evidence. There are no standards on how to present electronic evidence before the court.

Although laws are supposed to be technology-neutral, it is more apt to create new statutes that would be suitable to the developments in technology and in the way things are today. Failure to do so may lead to the injustice on the part of victims of cybercrimes, particularly of sex scandals – as they would not be able to prosecute the crimes committed against them successfully; and on the part of the accused in such cases – as there are not enough safeguards to protect their rights.

– o0o –