Cybercrime Safety of Women and Children: A Matter of Cyberspace Stakeholders' Ethics and Responsibility

Lizel Rose Q. Natividad, MA
San Beda College

I. Introduction

Development in technology has revolutionized the way the world mobilizes. Transfer of information could reach in various areas of the globe at a significantly speed and degree of efficiency. The world is becoming borderless in terms of information sharing and dissemination. On the other hand, this technological advancement in computer usage has been the target of abuse and misuse. Computers now raise special ethical issues, thus computer ethics warrants special status. The involvement of computers in human conduct can create entirely new ethical issues, unique to computing, that do not surface in other areas (Maner, 1996). Computer use has led to abuse, fraud, crimes, and catastrophes. Privacy is challenged and its definition is evolving. As a result, policies are continuously formulated and amended because of drastic technological changes. As computer systems become more complex, more ethical problems arise.

In a research conducted by Maner (1996), he discusses the unique properties of computers. Computers store information in forms of integers and that there is a possibility for this storage to be corrupted. Such corruption may result to collapse of an entire system, resulting to long period of manual operation. This may be seen when banks, for example, suddenly reports that an ATM account suddenly contains millions of pesos when the depositor has not done anything. Computers are logically malleable. They can be molded to do any activity in terms of inputs, outputs, and connecting logical operations. A person with physical disability may have his computer work with voice recognition software so that his input would not depend on keyboard or mouse anymore. Another unique property of computing machines is its superhuman complexity. Behaviors of programs produced can defy inspection and understanding. Computers are uniquely fast and cheap. Computers can perform millions of computations in a second at no cost. Lastly computer technology is discrete that small hidden applications such as bots can be sent by individuals and that it is uniquely cloned. Computers can make an exact copy of an artifact and the copy may be indistinguishable from the original. This property is very much observed in the Philippines, where pirated copies of software abound.

Computers have introduced multitude of developments in the growth of modern and complex communication technology, making life easier, but they have also brought about lots of concerns. Computer systems and their networks have deliberately enabled individuals commit crimes in fast and digital way. These crimes are referred to as cybercrimes.

The Philippines is not excluded in various acts of cybercrimes. Various news articles have published police operations raiding cyber stations employing mostly women and children to engage in international cybersex. Pirated DVDs proliferate in many areas of the country. These pirated DVDs usually feature women and children as sex objects. Moreover, online prostitution, real-time cyber pornography, and even deliberate uploading of obscene acts involving innocent women and children have been a major problem in the digital world. This paper intends to analyze and find ways to address the issue victimizing women and children through secondary research. Information and data collection are based from various scholarly studies, journal and news articles, and other publications. It first analyzes the special ethical issues related to computers and the nature of the cybercrimes, then it looks into the cybercrime phenomenon in the Philippines and look closer at how it affects women and children. It concludes with how the issue can be addressed.

II. Nature of Cybercrimes and the Computer Ethics

Cybercrime is broadly defined at the Tenth United Nations Congress on the Prevention of Crime and Treatment of Offenders by the Computer Crime Research Center as ‘any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or disturbing information by means of a computer system or network' (United Nations, 2000). Cybercrime is also referred to as computer crime, ICT crime, and high tech crime. The Philippine Department of Justice expands the definition by stating that 'a cybercrime is a crime committed with or through the use of information and communication technologies such as radio, television, cellular phone, computer and network, and other communication device or application (DOJ, 2012).

Singh & Geeta (2013) lists four major categories of cybercrimes. The first category is the cybercrimes against persons such as harassment via e-mails and social sites, cyber-stalking, defamation, hacking, cracking, e-mail spoofing, sms spoofing, carding or use of false ATM cards, cheating and fraud, child pornography, and assault by threat. The second category is the cyber crimes against property, which includes intellectual property crimes, cyber squatting, cyber vandalism, hacking computer system, transmitting virus, cyber trespass, and internet time thefts. The third category is cyber crimes against government and this includes cyber terrorism, wherein individuals and groups use the cyberspace to threated the international governments and/or the citizens of a country. The fourth category is cybercrimes against society at large, which affects large number of persons. Child pornography may also be under this category. Other types are cyber trafficking, online gambling, financial crimes, and forgery. In the study of Bossler and Holt (2010 as cited in Ngo & Paternoster, 2011), however, a subsequent factor analysis of forms of cybercrime result to two categories, namely person-based victimization (i.e., offenses where the individual was the specific target) and computer-based victimization (i.e., offenses where the individual was not the target but computers were).

The Information and Communication Technology (ICT) has perked-up economic and social opportunities in the advent of globalization, enabling individuals to cross borders and use computer systems in almost all aspects of the world's infrastructure sectors like banking, communications, energy, health, emergency services, agriculture, water supply, government services, manufacturing, strategic commercial centers and even religious and cultural institutions (Perante-Calina, 2012). But the advantages brought about by ICT have corresponding drawbacks, that's why many countries around the world are making efforts to gain cyber security. In 2013, the consumer cybercrime has had 378 million victims, causing damage that cost US $113 billion (Norton Cyber Crime Report, 2013 as cited in Heffron, 2014).

Associated with the cybercrimes is the principle of computer ethics. Computer ethics is defined as a "kind of professional ethics in which computer professionals apply codes of ethics and standards of good practice within their profession" (Stanford Encyclopedia of Philosophy, 2015). This also includes responsible use of computer and good internet behavior practices. Cybercrime violates the principle of computer ethics as it evades the basic rights on the protection and safeguard of computers, its systems, and related networks. Computer ethics goes against the violation of abuse, illegal access, misuse of computer and the use of internet. Consequently, computer ethics encompasses people who access and stream information. These users may not be the cybercrime perpetrators but they are also called to practice responsible digital behavior.

III. Cybercrime in the Philippines

The Philippines joins the move in strengthening the legal framework to address cybercrimes. Because of its discrete nature, cybercrimes have been difficult for law enforcement authorities to identify cybercriminals and the locus commissi delicti or place of the commission of the crime and tempus commissi delicti or time of the commission of the crime (Picotti et al., 2008 as cited in Perante-Calina, 2012).

In the Philippines, 87% of internet users were identified in 2010 report of the security software firm Symantec as victims of crimes and malicious activities committed online such as malware (virus and Trojan) invasion, online or phishing scams, sexual predation, and services in social networking sites like Facebook and Twitter. The Philippine National Police's (PNP's) Anti-Transnational Crime Division (ATCD) of the Criminal Investigation and Detection Group (CIDG) has confronted 2,778 referred cases of computer crimes from government agencies and private individuals nationwide from 2003 to 2012. The number of cases may be small considering that there may be many individuals who decide not to report the problem or simply do not know that such crime has been committed against them. (DOJ, 2012).

The first recorded cybercrime in the Philippines is that of Onel de Guzman, a young Filipino dropout, who created and released the "I Love You" virus, which attacked millions of Windows personal computers on and after May 5, 2000. When opened, the computer worm would do damage on the local machine, overwrite image files, and send copy of itself to all addresses in the address book. It caused damage to over 50 million computers of private and government institutions in Hongkong, Europe, and United States, amounting to US $5.5-8.7 billion to computer and additional US $ 15 billion to remove the worm (Sosa, 2013). The case filed against him was dismissed because there was no law punishing the deed as of that time.

One month after the worm outbreak, the Philippine government signed the Electronic Commerce Act of 2000 (Republic Act (RA) No. 8792) into law. The Philippines was third, next to Singapore and Malaysia, to enact an e-commerce law. The law penalizes hacking, cracking, and piracy. The law does not provide, however, penalties to other cybercrimes such as cyber-fraud and similar offences (Sosa, 2013)

The first Filipino to be convicted under Section 33a of the E-Commerce Law was JJ Maria Giner, who pleasded guilty to hacking the government portal "gov.ph" and other government websites. Giner was sentenced to one to two years of imprisonment and was fined P100,000. Remorseful Giner immediately applied for probation, which was eventually granted allowing him to skip jail time but would still be required to report to a probationary officer on a regular basis (Perante-Calina, 2012).

As of writing, the most widely used ICT is the social media, which is an online media that has the elements of participation, multiple conversations, openness to feedback, formation of communities, and connectedness (Mayfield, 2008 as cited in Cabalza & Domingo-Almase, 2013). Filipinos ranked first in social networking, sharing photos, and viewing videos, second to South Korea in reading blogs, second to Brazil in sharing videos, fourth in writing blogs and downloading podcasts, and sixth in using rich site summary or RSS feeds (McCann Universal, 2008 as cited in Cabalza & Domingo-Almase, 2013). In an investment analysis of Wall Street in 2011, the Philippines was proclaimed as the "Social Networking Capital of the World" (Cabalza & Domingo-Almase, 2013).

Aside from the E-Commerce Act of 2000, other cybercrime-related laws include the Anti-Trafficking in Persons Act of 2003 (RA 9208), Anti-Child Pornography Act of 2009 (RA 9725), Anti-Photo and Voyeurism Act of 2009 (RA 9995), and Cybercrime Prevention Act of 2012 (RA 10175).

Cybercrime Prevention Act of 2012 also known as RA 10175 is an act defining cybercrime, providing for the prevention, investigation, suppression, and the imposition of penalties. The law seeks to address issues concerning online information and interactions. But the passage of the Cybercrime Prevention Act of 2012 faced a total of 15 petitions filed before the Supreme Court. The petitions sought for nullity of questionable provisions especially the ones that suppress user's freedom of speech. On February 18, 2014, the Supreme Court upheld the legality of the Cybercrime Prevention Act (Rojas, 2014), which addresses cybercrimes such as hacking, identity theft, cybersex, child pornography, prostitution, libel, and the like.

While the Philippines faces issues in the legal arena, the more pressing issue is the lack of awareness and educational program for the citizenry and stakeholders. Victims may not be aware that they are victimized or they decide to remain silent because of distrust in the legal system. Many cybercrime perpetrators remain unpunished.

Mallari (2010, as cited in Perante-Calina, 2012, p. 33) summarized that from the perspective of law enforcement authorities, some of the limitations include: "1) the Internet Service Providers (ISP) under the law are not obliged to maintain important logs and cooperate with law enforcement in the investigation of computer crimes; 2) telecommunications companies are not obliged to cooperate with law enforcement in the investigation of computer crimes; 3) internet cafes/cyber cafes where most of the computer crimes perpetrators perform the violations are not obliged to maintain records of clients and customers; 4) other offenses committed with the use of computers and/or the internet are not penalized under said law like internet gambling, internet pornography, cyber terrorism.”

IV. A Focus on Cybercrime against Women and Children

To maximize the benefits of information and communication technology, the citizens need to be protected from cybercrimes. The rights-based approach pays special attention to the most vulnerable groups, which include women and children.

In 2007, the study conducted by the Council for the Welfare of Children (CWC) and the Philippine National Police (PNP) on the Modus Operandi of Perpetrators of Child Pornography in the Philippines was supported by the UNICEF. The said study showed the increasing syndicates of child pornography in cyberspace. UNICEF representative, Ms. Vanessa Tobin, mentioned that the Philippines is believed to be among the producers of pornographic material involving young kids, which is sent in various areas in the world, mostly via the internet (UNICEF, 2009).This became among the precursors for the passage of the RA 9775 or the Anti-Child Pornography Act and the Anti-Photo and Voyeurism Act of 2009 (RA 9995). Amidst the enacted of the law, the Philippines is still plagued with online pornography involving children. NBI Anti-Human Trafficking Division chief Dante Bonoan reported that said syndicated is widespread and become a “cottage industry”, meaning online pornography in moving to different homes to create cybersex dens. He even reported that these activities have reached the international investigation such as in the United Kingdom and the USA (rappler.com,2015).

Other than the cyber abuses on children, women are also victims of cybercrimes. In 2013, a close coordination between the US and the Philippine governments successfully busted cybersex den in Central Luzon where minors and women were subject of pornography and sexual exploitation (Manila Bulletin, 2013). Representatives of women’s party-list group Gabriela, Luzviminda Ilagan and Emmi de Jesus, filed proposed amendments to the Anti-Violence Against Women and Children Act (VAWC) or RA 9262 through House Bill (HB) 6815. The proposed amendments include violence against women (EVAW) as punishable by law. If passed, the house bill will include EVAW, which covers all "acts that use ICT which cause or are likely to cause mental, emotional, or psychological distress to the victim," as criminal offense (Esteban, 2013).

Gabriela Internal Deputy Secretary General Gertrudes Libang said that the provisions of the Cybercrime Law for sexual content penalizes those in sex videos, whether or not the videos were uploaded with consent, and not those who uploaded the content. Women are twice disadvantaged for the social embarrassment brought about by the video and for being penalized because of the uploaded video. Libang added that if the amendments will not be passed, then no law will defend the victims of EVAW. Those who upload sex videos featuring women and children are considered abusers of women and children and should not be immuned from punishment (Esteban, 2013).

Children, on the other hand, learn and play in the cyberspace. Gadgets are provided for children for educational and recreational purposes and because of this, they are also exposed to mobile internet access, instant messaging, mobile web cam, internet relay chat (IRC), peer-to-peer newsgroups, bulletin boards and file sharing. Thus, they are open to threats such as online bullying, identity thefts, cyber staking, child predators, sex offenders and child pornography (Hussain, 2011).

Cyberspace poses great harms especially to children because its boundaries are unrecognizable. Sources of threat are difficult to identify because they can operate from far off places. The concern is not only national, but transnational, thus the initiative should be global, having joint venture with ECPAT (End child Prostitution, Child Pornography, and Trafficking of Children for Sexual Purpose) and UNICEF for violence against children in Cyberspace (Hussain, 2011).

Hussain (2011) enumerates other factors contributing cybercrimes against children. One is the ubiquitous access to the internet, making access to computers very easy to children, which also make them easy prey to cybercrime perpetrators. Another factor is the massive production and distribution of pornographic images. They are easily available in social media such as Facebook and Twitter, which children now use. Third is commercialization of websites that deal with child pornography and other unsolicited activities. Fourth is the ignorance toward cybercrimes, which will be dealt with in this paper further in the last part. The public lacks education on the harmful consequences of cyber crimes. Next are lack of legislative framework and lack of cyber forensic abilities or the ability to extract information and date from computer storage media in order to capture cyber criminals. Another reason is lack of information technology training among prosecutors and judges who rely heavily on cyber experts' assistance. Lastly, there is also inadequate crime reporting procedure.

V. Preventing Cybercrime

The study of Ngo and Paternoster (2011) explored the effects of individual and situational factors on seven forms of cybercrime, namely, computer virus, unwanted exposure to pornographic materials, sex solicitation, online harassment by a stranger, online harassment by a nonstranger, phishing and online defamation. Several studies (Choi, 2008; Bossler & Holt, 2009; Holt & Bossler, 2009; Marcum, 2008 as cited in Ngo & Paternoster, 2011) reveal that engaging in online risky behaviors and activities such as downloading free games and free music at unknown websites, opening unknown email attachments, clicking on pop-up messages, spending time in chat rooms, and using Instant Message (IM) chat significantly increase the likelihood of online victimization. Nevertheless, general computer use and activities such as playing video games, shopping, or checking e-mail did not have significant impact on the likelihood of experiencing online harassment (Holt and Bossler, 2009 as cited in Ngo & Paternoster, 2011).

Bossler and Holt (2010 as cited in Ngo & Paternoster, 2011) assessed the effects of self-control on the probability of experiencing five forms of cybercrime victimization: unauthorized access to one's computer, having information added, deleted or changed on one's computer without knowledge or permission, data loss due to malware infection, having one's credit card information electronically obtained without knowledge or permission, and online harassment. The authors found low levels of self-control were significantly related to the likelihood of experiencing three of the five forms of cybercrime victimization – unauthorized access to one's computer, having information added, deleted or changed on one's computer without knowledge or permission, and online harassment.

Criminals look for easy prey and they include women and children. The general public, especially women and children, need to be properly educated on the incapacitating effect of cyber crimes and improper computer ethics. They need to be more aware of the dangers of cybercrime and at the same time should be educated on becoming ethical users of computers and information systems. The public should understand its role in the country's cybersecurity (Sosa, 2013).

The public may be educated using the five main categories of particular interest to technologists -- privacy, ownership, control, accuracy, and security (Relkin, 2006). How much information should one divulge in public so as not to have problems in personal security? Information such as compensation, background data, personal identification information such as social security number and account identifiers should not be easily accessible to the public and should not be entered in computers accessed by the public.

Personal outputs, pictures, and videos are matters of ownership. To protect them from abuse, individuals should learn not to make them accessible to everyone. Most especially children should be protected from internet sites that could be harmful to them. This can be done by monitoring their internet activities and blocking sites that are potentially damaging to them.

As found of Bossler and Holt (2010), a good amount of self-control is needed to lower the probability of being victimized in cyberspace. The public should be taught to refrain from risky online behaviors such as downloading free games and free music at unknown websites, opening unknown email attachments, clicking on pop-up messages, spending time in chat rooms, and using Instant Message (IM) chat.

Security measures can be taught to the public too. Logging out especially from online banking and shopping protects one from possible hackers who will use the account. Likewise, tabbed browsing should not be used when doing online banking. As much as possible online banking and shopping should be done in personal computers, not in public computers. It also pays to clear the cache on the computer to prevent others from seeing the last pages visited. These are but simple security measures. The public can be even further educated of technologically advanced safeguards such as SSL and encryption, firewall, monitoring, and automatic logout.

Most importantly, the public should also be educated of basic IT ethics to guide everyone about data or computer usage. While everyone may be a potential victim, everyone may also become potential perpetrators of cybercrime. Because it is a serious offense, safeguarding the safety of the public especially of children and women is a great responsibility of cyberspace stakeholders. The government has also an important part for the prevention of cybercrimes. PNP-ACG maintains Cyber-Patrolling and Terror Response Team for the monitoring and production of social media exploitation made by Persons of Interest (POI). Also the Project AngelNet of the Philippine Government specifically focuses on an information dissemination campaign for the protection of women and children from the menace of online abuse (Department of Justice, 2015).

Website and Internet resources can be the main venue for information source. Media can play its role by broadcasting information campaign. Schools can have campaigns to boost awareness. Once parents are teachers are educated regarding the dangers of cyber crime and how to deter them, they are able to protect their children.

VI. Conclusion

Protection of women and children is of great concern because they are easy preys for abuse. This is the reason why some groups such as Gabriela work towards amending laws that do not further victimize women and children. While change in legal infrastructure is sought after, something else can be done and that is strengthening the ethical responsibility of the cyberspace stakeholders such as Internet service providers, software designers, webhosts, cyber café owners, and the like. Each one has personal responsibility and everyone cannot just depend on law enforcers. There can be own level of policing, not tolerating and blocking possible offenders.

REFERENCES

Avedano, C.O. (January 1, 2013). *87% of Filipino Internet users have been victims of cybercrimes–DOJ. Inquirerdotnet.* Philippine Daily Inquirer. Retrieved on November 21, 2014 from http://technology.inquirer.net/21557/87-of-filipino-internet-users-have-been-victims-of-cybercrimes-doj#ixzz3K9Zrc0T7

Cabalza, C.B. & Domingo-Almase, A.D. (July 12, 2013). *Trends and Threats in Cyberspace: Are We Secure?.* National Defense College of the Philippines (NDCP) Policy Brief. No. 11 www.ndcp.edu.ph.

Department of Justice (DOJ) (2012). *Primer on Cybercrime. Retrieved* November 21, 2014 from http://www.doj.gov.ph/files/2012/Primer_on_Cybercrime.pdf

Department of Justice (DOJ). Philippines 2014-2015 *Cybercrime Report. The Rule of Law in Cyberspace,* 15, March 2015. Retrieved April 2015 from https://www.doj.gov.ph

Esteban, J.M. (January 24, 2013). I*nstead of Cybercrime provisions, Gabriela pushes for revised law on violence against women.* Philippine Collegian (22).

Heffron, J.K.C. (February 2014). *Boon or bane: Business and the anti-cybercrime law.* DLSU Business Notes and Briefings. (4) 2: 1-4.

Hussain, R. (March 2, 2011). *Cyberspace Task Force for Child Protection.* International Journal of Academic Research (3) 2: 1001-1007.

Libel and cybercrime laws in the Philippines. Retrieved November 21, 2014 from http://freespeechdebate.com/en/media/marites-vitug-interview/

Maner, W. (April 1996). *Unique Ethical Problems in Information Technology. Science and Engineering Ethics,* (2) 2: 137-154.

McConnell International LLC (December 2000). *Cyber Crime ... and Punishment?:* Archaic Laws Threated Global Information. Retrieved on November 21, 2014 from www.mcconnellinternational.com/ereadiness/report.cfm.

NBI: Online sex trade cottage industry in PH. Retrieved April 27, 2015. www.rappler.com.

Ngo, F.T. and Paternoster, R. (January-July 2011). *Cybercrime Victimization: An examination of Individual and Situational level factors.* International Journal of Cyber Criminology (5) 1: 773-793.

Philippines: Anti-Cybercrime Law Denounced as 'Cyber Martial Law'. January 21, 2013. Retrieved November 21, 2014 from http://globalvoicesonline.org/2013/01/21/philippines-anti-cybercrime-law-denounced-as-cyber-martial-law/

PH-US team busts Luzon-based Cybersex Ring. Manila Bulletin, August 22, 2013.

Perante-Calina, L.E. (2012). *Addressing cybercrimes in the Philippines: A legal framework is crucial.* A policy paper submitted to UP-NCPAG as part of the course requirement in PA 247 (Policy Paper), SY 2011-2012.

Relkin, J. (August 15, 2006). 10 *ethical issues confronting IT managers.* Retrieved November 21, 2014 from http://www.techrepublic.com/article/10-ethical-issues-confronting-it-managers/

Rojas, V. (February 21, 2014). *Supreme Court: Cybercrime Prevention Act Constitutional.* Retrieved November 21, 2014 from http://www.

ambibo.com/news/supreme-court-cybercrime-prevention-act-constitutional/

Singh, H. & Geeta, D. (May 2013). *Cyber Crime – A Threat to Persons, Property, Government and Societies.* International Journal of Advanced Research in Computer Science and Software Engineering (3) 5: 997-1002

Sosa, G.C. (January 2013). *Country Report on Cybercrime: The Philippines. 140th International Training Course Participants' Papers.* Resource Material Series No. 79. Retrieved November 21, 2014 from http://www.unafei.or.jp/english/pdf/RS_No79/No79_12PA_Sosa.pdf

Stanford Encyclopedia of Philosophy. Retrieved April 27, 2015. http://plato.stanford.edu/entries/ethics-computer/.

UNICEF, *Child Rights Actors Call for Immediate Passage of Anti-Child Pornography Bill.* Retrieved April 27, 2015. http://www.unicef.org/philippines/8891_10695.html.

United Nations (2000). *Vienna Declaration on Crime and Justice: Meeting the Challenges of the Twenty-first Century. Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders.* Vienna, 10-17 April 2000. Retrieved November 21, 2014 from http://www.uncjin.org/Documents/congr10/4r3e.pdf