MY MOTHER, MY PIMP: JURISDICTIONAL AND EVIDENTIARY ISSUES IN PROSECUTING INTERNET-FACILITATED SEX TRAFFICKING*

*Paula P. Plaza***

ABSTRACT

The Philippines is among the top ten source countries in the world for internet-facilitated sex trafficking, which includes cybersex and child pornography. In many cases, the biological parents or relatives themselves prostitute their own children, nephews, or nieces to sex offenders abroad. To address this issue, as well as other internet-related offenses, the Philippine Congress passed the Cybercrime Prevention Act in 2012. Despite this law, however, cybersex and child pornography remain prevalent. Using a blended methodology of key informant interviews and extensive literature review, this Article explains into the jurisdictional and evidentiary issues that hinder the effective enforcement of the Act. The author recommends that the country accede to the Budapest Convention; enter into more mutual legal assistance treaties (MLATs); extend the coverage of the listed crimes in existing MLATs; make more aggressive use of current MLATs; enter into more bilateral extradition treaties; expand the crimes listed in existing treaties; amend the provision in the Expanded Anti-Trafficking in Persons Act on extraterritoriality to fit the principle of dual criminality; and include cybersex within the ambit of continuing crimes.

> *"Perhaps when people hear about cybersex they think it doesn't have any physical effect [...] But it can do things to your core. It can take things from you, your dignity and your purity."*
>
> —Shaina, a 15-year old victim[1]

---

* *Cite as* Paula Plaza, *My Mother, My Pimp: Jurisdictional and Evidentiary Issues in Prosecuting Internet-Facilitated Sex Trafficking*, 89 PHIL. L.J. 687, [page cited] (2015).

** J.D., University of the Philippines College of Law (2015); B.A. Major in Sociology, Minor in Political Science, McGill University (2010). Best Speaker in the Preliminary Rounds of both the South East Asia Regional Rounds (2013) and International Rounds (2014), Stetson International Environmental Law Moot Court Competition.

I. Introduction

Internet-facilitated sex trafficking in the form of cybersex and child pornography are perpetrated in more than a third of the country's provinces, affecting tens of thousands of Filipino families.[2] Notwithstanding the fact that the perpetrator never lays a hand on the victim, their pernicious effects are real. Numerous psychological studies, for example, consistently show that victims of online sexual abuse suffer from severe personality disorders, substance abuse, and mental health problems.[3] These consequences are exacerbated in the Philippine setting where it is common that the biological parents or relatives themselves "sell" the "services" of their own children, nephews, or nieces. The blood relationship magnifies the terror, and ensures continued access to the victim.

According to the records of the Philippine National Police-Anti Cybercrime Group, 2,260 cybercrimes were committed and reported in the past five years, and the number of crimes that target women and children are on the rise.[4] Left unchecked, these cybercrimes will continue to escalate as internet connectivity increases, especially in light of the fact that internet usage in the country grew by 531% within the same period.

This Article seeks to address the reasons why cybersex and child pornography are still prevalent in our country despite the passage of R.A. No. 10175 or the Cybercrime Prevention Act in 2012. Using a blended methodology of key informant interviews and extensive literature review,[5] the

---

The author would like to extend her deepest gratitude to her advisor in the Supervised Legal Research class, Prof. Rommel J. Casis and her professor in Evidence, Prof. Carlos Roberto Z. Lopez.

[1] Name changed for protection.

[2] *See* Appendix A, "PNP Anti-Cybercrime Group – Cybercrime Offenses in the Philippines from 2010-2014."

[3] *See* Part II(A), *infra.*

[4] *Supra* note 2.

[5] The research output and recommendations are the result of five focus interviews with experts in the field of cybercrime given the novel nature of the topic and the need for practical guidance and actual statistics. These experts are the Assistant Secretary of the Department of Justice ("DOJ") who is concurrently the Head of the Office of Cybercrime, the Chief of the Web Services and Cyber Security Division of the Philippine National Police ("PNP"), the Deputy Executive Director of the Information and Communications Technology Office-Department of Science and Technology ("ICTO-DOST") and a member of the National Advisory Council of the PNP Anti-Cybercrime Group. To gain more hands-on knowledge and practical application of the rules on electronic evidence, the author also met with a digital forensic investigator from the National Bureau of Investigation ("NBI") -

Article examines various issues in evidence and jurisdiction related to the Act that stand as a challenge towards effective law enforcement.[6]

This Article demonstrates that there is ineffective implementation of the Cybercrime Prevention Act, particularly in prosecuting offenders, because Philippine jurisprudence on electronic evidence is largely undeveloped and there is confusion on the proper application of the rules and authentication of evidence. Similarly, the acquisition of information and jurisdiction is difficult due to the transnational nature of the crime and that fact that majority of the offenders never set foot on Philippine soil.

In light of these identified problems, the Article forwards several recommendations. With respect to jurisdiction, the author recommends that the country 1) accede to the Budapest Convention; 2) enter into more mutual legal assistance treaties ("MLATs"); 3) extend the coverage of the listed crimes in existing MLATs; 4) make more aggressive use of current MLATs; 4) enter into more bilateral extradition treaties; 5) extend the coverage of the listed crimes in existing treaties; and 6) amend Section 26-A of Rep. Act No. 9208, as amended by Rep. Act No. 10364 or the Expanded Anti-Trafficking in Persons Act, on extraterritoriality to fit the principle of dual criminality and to include cybersex within the ambit of continuing crimes.

With regard to evidence, the author drafts a basic framework module that may be used to guide prosecutors on the fundamental rules of authentication of electronic evidence. The framework consists of two parts, the first part lists the common forms of electronic evidence used in internet-facilitated sex trafficking, and their proper classification and mode of authentication under the Supreme Court Rules on Electronic Evidence.[7] The second part is a comprehensive summary of how authentication was performed in Philippine and United States cases with an analysis on how the American cases can be applied in the Philippines to combat internet-facilitated sex trafficking.

Computer Crimes Unit ("NBI-CCU") who was presented as an expert witness on cybercrime for several trials.

The author also examined existing laws, Philippine MLATs, bilateral and multilateral extradition treaties to which the Philippines is a state party, DOJ annual reports from 2002-2013, Philippine jurisprudence applying the rules of electronic evidence from 1999-2014, and selected U.S. cases on electronic evidence.

[6] This Article is focused on involuntary and coerced cybersex, it excludes cybersex between consenting adults of legal age, and cybersex with avatars or computer-generated and digitally crafted images. Although the topic of avatars is an important issue, it raises important issues on freedom of expression and the appropriate extent of regulation, which the author could not adequately discuss given the limited scope of this paper.

[7] A.M. No. 01-7-01-SC, July 17, 2001.

II. Cybersex as a Crime in the Philippines

A. The use of the internet as a means of committing crimes

Cybercrime is an umbrella term used to identify criminal activity that is committed through a computer or a computer network.[8] It is one of the fastest growing non-violent crimes in the Asian Region,[9] and globally, the cost of malicious cyber activity is estimated to be between USD 300 billion and USD 1 trillion.[10] Unfortunately, there is a positive correlation between the rise in internet usage and cybercrime incidents.[11] Increased internet access can translate to a greater demand for cybersex and child pornography, for which the Philippines is an established source country.[12] This underscores the need for an effective legislative and enforcement system to combat these crimes. In the Philippines alone, internet usage grew by 531% in the past five years.[13] This is practically double of the worldwide growth of internet usage pegged at 249% in the last seven years.[14]

Why is there a positive correlation between internet usage and cybercrime? One psychological study, outlining the factors that make the internet alluring for sexual predators, suggested that the internet provides a convenient method for cybersex predators to indulge in their deviant behavior. First, the internet provides them with anonymity. They may assume different "handle names" online, and are virtually untraceable. Individuals are "more inclined to behave deviantly given disinhibition, anonymity and depersonalisa-

---

[8] *See* DAVID S. WALL, THE TRANSFORMATION OF CYBER CRIME IN THE INFORMATION AGE 10 (2007); Mike McGuire & Samantha Dowling, *Cyber Crime: A Review of the Evidence Research Report, Summary of Key Findings and Implications*, United Kingdom Home Office Research Report No. 75 (Oct. 2013), at 6, *available at* https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf; Robert Moore, Investigating High-Technology Computer Crime 4 (2010).

[9] Gilbert Caasi Sosa, *Country Report on Cybercrime: The Philippines*, UN Asia and Far East Institute for the Prevention of Crime and Treatment of Offenders Resource Material Series No. 79 (Dec. 2009), at 80, *available at* http://www.unafei.or.jp/english/pdf/RS_No79/No79_00All.pdf.

[10] *See* MAJID YAR, CYBERCRIME AND SOCIETY 15 (2013); Chris Hale, *Cybercrime: Facts and Figures Concerning This Global Dilemma*, 18 CRIME & JUST. INT'L 24, 26 (2002).

[11] Interview with Atty. Geronimo Sy, Assistant Secretary of the DOJ, Head of the Office of Cybercrime (Feb. 11, 2015).

[12] *Id.*

[13] Jason Mander, *As the Internet Turns 25, China Has 2.5 More Users Than The US*, GLOBAL WEB INDEX, Mar. 12, 2014, *available at* http://www.globalwebindex.net/blog/internet-turns-25.

[14] *Id.*

tion online."[15] Second, the internet allows them to groom multiple victims at the same time through different websites or online services. The predator can engage in as many conversations and transactions as he/she wishes as long as he/she has enough means to pay for it. This is in contrast to conventional sex trafficking where the perpetrator generally meets a single victim during an encounter. Third, services acquired through the internet require less time and resources than actually traveling to the location and being physically present in the area. Fourth, technological advances allow the perpetrator to keep his or her files confidential and out of reach from family and co-workers. There is less likelihood of discovery and they can easily record and copy the files for later viewing.[16]

With the exponential growth in internet usage, cases similar to *United States v. Pavulak*[17] may be replicated on an even larger scale. Pavulak was based in Delaware. Through the use of a website and email, he was able to establish a connection with the mother of a two-year-old child in the Philippines. He sent her cash through online money transfers and provided the mother with a webcam-enabled laptop so he could view the child's genitals. Later, he flew to the Philippines and produced a video of himself and the mother engaged in explicitly sexual conduct. He described it as a 'training video' for the two-year-old.

Another similarly harrowing example is the case of *United States v. Mathias*,[18] where a man based in Florida was able to get in touch with a mother of minor daughters, aged 11 and 12, through a website. Mathias and the mother exchanged hundreds of emails to iron out the details of the transaction. In January 2014, officers in Taguig, Philippines arrested a mother who charged her foreign clients so they could watch her daughter strip in front

---

[15] M. Aiken, M. Moran & M. J. Berry, *Child Abuse Material and the Internet: Cyberpsychology of Online Child Related Sex Offending*, Paper presented at the 29th Meeting of the INTERPOL Specialist Group on Crimes Against Children (Sept. 2011), at 4-7; PAUL E. MULLEN, MICHELE PATHÉ & ROSEMARY PURCELL, STALKERS AND THEIR VICTIMS 59 (2009); Leroy Macfarlane & Paul Bocij, *An Exploration of Predatory Behavior in Cyberspace: Towards a Typology of Cyberstalkers*, 8 FIRST MONDAY 15 (2003).

[16] Arthur Bowker & Michael Gray, *The Cybersex Offender and Children*, 74 FBI L. ENFORCEMENT BULL. 12, 13-14 (2005), *available at* https://leb.fbi.gov/2005-pdfs/leb-march-2005.

[17] 672 F. Supp. 2d 622 (D. Del. 2009), *cited in* Anitha S. Ibrahim, Ed McAndrew & Wendy Waldron, *Emerging Issues in the Extraterritorial Sexual Exploitation of Children Sexual Exploitation Crimes Against Children*, 59 UNITED ST. ATTORNEY'S BULL. 59, 59 (2011), *available at* http://www.justice.gov/sites/default/files/usao/legacy/2011/09/08/usab5905.pdf

[18] No.09-cr-60292 (S.D. Fla. 2010), *cited in* Ibrahim et al., *id.* at 59.

of a web camera.[19] In cases such as this, the offenders can make sexual requests from the victims and their pimps from the comfort of their homes. The predators may remain abroad, but the effects reverberate across oceans, in violation of Philippine laws explicitly prohibiting such acts. The internet emboldens the predator[20] and creates a continuing demand to the detriment of Filipino men, women, and children.

B. The prevalence of internet-facilitated sex trafficking or cybersex in the Philippines

By no means is this crime isolated and sporadic. It affects thousands of Filipino families, and has serious implications that affect the socio-psychological development[21] and well-being of both victims and their families.

Senior Supt. Gilbert Sosa, head of the Philippine National Police (PNP) Anti-Cybercrime Unit, stated that the Philippines is among the "top ten" purveyors of a global "cottage industry [worth] billions of dollars." Cybersex is performed in more than a third of the Philippines' provinces, "with Angeles, the central city of Cebu, and the southern city of Cagayan de Oro being the other main sites."[22] Ruby Ramores, a former executive of the Inter-Agency Council Against Child Trafficking forwards that "tens of thousands of women are involved in the industry and that most of the girls are recruited by friends, family."[23]

Unfortunately, the official statistics of the PNP Anti-Cybercrime Group do not provide a complete picture of the prevalence of cybercrimes in the country, particularly of internet-facilitated sex trafficking. To illustrate, of the 32 complaints brought before the Women and Children Protection Section of the PNP Anti-Cybercrime Group in 2013, 43% of complainants

---

[19] *Mom Peddles Own Daughter in Cybersex Ring*, ABS-CBN NEWS ONLINE, Aug. 8, 2014, http://www.abs-cbnnews.com/video/nation/metro-manila/08/06/14/mom-peddles-own-daughter-cybersex-ring.

[20] WALL, *supra* note 8, at 32.

[21] Sigríður Sigurjónsdóttir, *Consequences of Victims' Mental Health after Internet-initiated Sexual Abuse: a Sexual Grooming Case in Sweden*, Master's Thesis, Stockholm University Department of Psychology (2012), at 8-9, *available at* http://www.diva-portal.se/smash/get/diva2:609191/FULLTEXT01.pdf.

[22] Agence France-Presse, *Philippines a Global Source for 'Cybersex' for Child Industry - Police*, RAPPLER, Jan. 17, 2014, *at* http://www.rappler.com/nation/48262-ph-source-child-cybersex-industry.

[23] Sunshine de Leon, *Cyber-sex Trafficking: A 21st Century Scourge*, CNN, July 18, 2013, *at* http://edition.cnn.com/2013/07/17/world/asia/philippines-cybersex trafficking.

did not return after they were advised to submit additional evidence.[24] This is attributed to the general fear and mistrust of technology, the perceived difficulty of obtaining evidence of the crime, and reluctance to prosecute.[25]

The difficulty of obtaining accurate statistics is due to several factors. First, in several cases, the biological parents or relatives were the sellers of the services of their children, nephews or nieces. In 2011, National Bureau of Investigation (NBI) agents raided a home in Cordova, Cebu City where six children aged four to fifteen years old were rescued and put in the custody of the Provincial Women's Commission. For three years, they were forced by their parents to provide online sexual performances. The cybersex business began after both their parents lost their jobs.[26] In another case, Timothy Ford, a resident of the Northamptonshire in the United Kingdom was convicted in 2013 for 23 offenses ranging from paying for sexual services of a minor to arranging and facilitating the prostitution of a child. During the investigation, files discovered on his computer showed that he would make money arrangements with the mother of the boys, who would coerce her sons to perform 'shows' for him. Ford paid her as little as GBP 13 per hour.[27]

Most of the victims in these cases are minors. After the prosecutors file the complaint, the minors are coerced to file an affidavit of desistance. In instances where the minors refuse to file the affidavits, their parents or legal guardians execute the affidavit themselves. To combat this, the Department of Justice ("DOJ") issued a resolution in 2010 with consolidated guidelines on the prosecution of cases involving trafficking in persons. Prosecutors were instructed not to dismiss cases based on the mere execution of an affidavit of desistance and were instructed to "vigorously oppose and/or manifest strong objections to the motions for dismissal."[28]

---

[24] Interview with P03 Fuentes, Investigator, Women and Children Protection Services ACOTD (2011); Interview with Angel Redoble, Member, National Advisory Council of the PNP Anti-Cybercrime Group (Jan. 13, 2015).

[25] Interview with Joey Narcisco, Digital Forensic Investigator, NBI-Computer Crimes Unit (Feb. 18, 2015).

[26] *Parents Pimp Own Kids for Sex*, ABS-CBN NEWS, June 15, 2011, *at* http://www.abs-cbnnews.com/nation/regions/06/15/11/parents-pimp-own-kids-cybersex.

[27] Angus Crawford, *Philippines Web Abuse Ring Smashed in UK Operation*, BBC, Jan. 6, 2014, *at* http://www.bbc.com/news/uk-25749326; Kristen Schweizer, *Banks Help Cops Follow the Hidden Money Trail to Nab Pedophiles*, BBC, July 29, 2014, *at* http://www.businessweek.com/news/2014-07-28/pedophiles-nabbed-as-banks-join-cops-to-follow-the-money-trail#p1.

[28] DOJ Circular No. 57, July 29, 2010. *See* also Rep. Act No. 10364 (2013), An Act Expanding Republic Act No. 9208 [hereinafter "Expanded Anti-Trafficking in Persons Act"], § 11.

Second, due to the clandestine nature of sex trafficking, most victims would rather keep silent about their experiences. The fear of reprisals from recruiters and stigmatization[29] prevent victims from coming forward and prosecuting their case.

Lastly, the lack of knowledge on gathering electronic evidence to prove sex trafficking and sex crimes on the internet leads to a stagnation in the case after initial reporting.[30] The victims often do not return after being advised to come back with more evidence.[31]

C. The Cybercrime Law and the continuing rise of cybersex incidents

The official statistics provided by the PNP Anti-Cybercrime Group do not indicate the specific acts committed, whether these involved cybersex, or the ages of the victims. However, the clear trend is that out of the recorded 2,260 cybercrimes committed in the past five years, the number of crimes that target women and children are on the rise.

The acts committed in violation of the Anti-Photo and Video Voyeurism Act doubled from 36 in 2013 to 60 in 2014. From zero prosecutions for violation of the Anti-Child Pornography Act ("ACPA"), there was a sudden rise to 18 in two years. We see the same trend in the Anti-Violence Against Women and Children Act, from zero instances in 2010-2012, to six in 2013 and eight in 2014. It cannot be discounted, however, that the increase in numbers could also be the result of a sudden decongestion of cases, or a rise in the skill level of prosecutors who have become more adept in handling cybercrime cases.

The number of internet-facilitated sex trafficking crimes in the country will continue to rise if left unchecked. Atty. Geronimo Sy, Head of the Office of Cybercrime, and Assistant Secretary of the DOJ, stated that there are several reasons to buttress this prediction: (1) increased access to the internet; (2) high English proficiency of Filipinos; (3) poverty; (4) lack of education of victims who do not have an extra skill set; (5) a rise in global awareness of the Philippines; and (6) more inbound and outbound flights to the country.[32]

---

[29] Rowena Guanzon & Charmaine Calalang, *The Anti Trafficking in Persons Act of 2003: Issues and Problems*, 30 IBP L.J. & MAG. 70 (2004).

[30] Redoble, *supra* note 24.

[31] Fuentes, *supra* note 24.

[32] Sy, *supra* note 11.

In response to the growing problems, on September 2012, R.A. No. No. 10175 or the "Cybercrime Prevention Act of 2012" was signed into law. The constitutionality of majority of the provisions was upheld by the Supreme Court in *Disini v. Secretary of Justice.*[33] R.A. No. 10175 punishes cybersex[34] and child pornography[35] as content-related offenses.

D. Internet-facilitated sex trafficking as a crime and the problems in its successful prosecution

With respect to child pornography, the elements in R.A. No. 10175 are identical with the ACPA. However, the former increased the penalty for online child pornography by one degree due to the potential for uncontrolled proliferation. As noted by the court in *Disini,*[36] no one has questioned the provision on child pornography in the ACPA, thus the author will no longer discuss the rationale for criminalizing it.

Specifically, criminalizing cybersex is an audacious move on the part of Philippine legislators. The Budapest Convention, the law after which R.A. No. 10175 was modeled, does not mention cybersex as one of the content-related offenses. The criminalization of the offense in the Philippines can be understood by looking at the situation in our country. The Philippines is a top ten source country for the act. Cybersex is performed in 31 of the country's 81 provinces,[37] and more often than not, it is the biological parents, legal guardians and relatives who actually pimp the services of their kin.[38]

1. Rationale for Criminalizing Cybersex

The petitioners in *Disini* sought to strike down the prohibition on cybersex because it curtails legitimate behavior between husband and wife, and consenting adults. In resolving the challenge, the Supreme Court referred to the intent of the legislators shown in the deliberations of the Bicameral Committee of Congress to address cyber prostitution, white slave trade, and pornography for favor and consideration.[39]

---

[33] Disini v. Secretary of Justice, G.R. No. 203335, 716 SCRA 237, Feb. 11, 2014.

[34] Rep. Act No. 10175 (2012), § 4(c)(1). Cybercrime Prevention Act of 2012.

[35] § 4(c)(2).

[36] *Disini,* 716 SCRA 237.

[37] Agence France-Presse, *supra* note 22.

[38] Redoble, *supra* note 24.

[39] *Id.*

During the Senate deliberations, Senator Miriam Defensor Santiago expressed her apprehension and the need to revisit the definition of cybersex in R.A. No. 10175, primarily because the offense of cybersex was not included in the Budapest Convention for Cybercrime, but also because sex and obscenity are not synonymous.[40] In brushing aside subjective issues on obscenity and prior restraint, Senator Edgardo Angara explained that the crux of the cybercrime was that the act was done for money, consideration or favor. With a vote of 13-1, the Senate approved Senate Bill No. 2796, or the Cybercrime Prevention Act of 2012. Senator Teofisto Guingona III was the lone dissenter, he declared that he voted against the bill primarily because the definition of cybersex smacks of prior restraint, and legislates morality.[41]

Why would Philippine legislators go so far as to criminalize cybersex? A central question is whether harm is actually committed even though the perpetrators are hundreds of thousands of miles away, often in other continents. Despite the fact that the perpetrator never actually lays a hand on the victim, the effects are real.[42]

According to a 2012 study conducted by Sigríður Sigurjónsdóttir of the Stockholm University Department of Psychology, sexual abuse through the internet can lead to severe personality disorders and serious disruptions in the emotional development and self-esteem of survivors. Furthermore the victims undergo extreme feelings of shame and guilt, they often blame themselves for the abuse, which translates into maladaptive behaviors in their friendships and romantic relationships.[43] In a study conducted by Rogland and Christensen in 2010, they found that the victims are often at a loss with how to cope with the experience, and this often leads to substance abuse and mental health problems.[44] It cannot be denied that these problems will be compounded in the Philippine setting, where it is the guardians and biological kin who actually induce the children to engage in these acts.

2. Elements of the Crime of Internet-Facilitated Sex Trafficking

The crime of internet-facilitated sex trafficking is not novel, the use of the internet merely broadens the scale and reach of the traditional crimes of sexual exploitation. For the purposes of this Article, the author discusses

---

[40] Gonzales v. Katigbak, G.R. No. L-69500, 137 SCRA 717, July 22, 1985.

[41] *Id.*

[42] ERICKA RODAS, THE MULTI-FACETS OF CYBERSEX. A CALL TO ACTION AND REFORM FOR SOCIETY 12 (2014).

[43] Sigurjónsdóttir, *supra* note 21, at 8-9.

[44] *Id.*

the crime of sex trafficking in the form of (1) child pornography, and (2) cybersex, both of which are facilitated by the use of the internet and communication technology. To clarify the discussion, and to avoid any confusion in terminology, the elements of the crimes of (1) trafficking in persons, (2) cybersex, and (3) child pornography are detailed below.

The elements of trafficking in persons are enumerated in R.A. No. 10364, to wit:

> (a) *Trafficking in Persons* – refers to the recruitment, obtaining, hiring, providing, offering, transportation, transfer, maintaining, harboring, or receipt of persons; with or without the victim's consent or knowledge; within or across national borders; by means of threat, or use of force, or other forms of coercion, abduction, fraud, deception, abuse of power or of position, taking advantage of the vulnerability of the person, or, the giving or receiving of payments or benefits to achieve the consent of a person having control over another person for the purpose of exploitation; [exploitation] which includes at a minimum, **the exploitation or the prostitution of others or other forms of sexual exploitation,** forced labor or services, slavery, servitude or the removal or sale of organs.
>
> The recruitment, transportation, transfer, harboring, adoption or receipt of a child for the purpose of exploitation or when the adoption is induced by any form of consideration for exploitative purposes shall also be considered as 'trafficking in persons' even if it does not involve any of the means set forth in the preceding paragraph.[45]

The gravamen of the offense is the exploitation of the victim. This statutory provision and the case of *People v. Solemo*[46] provide basis to argue that cybersex and child pornography are forms of trafficking in persons, since the purpose is sexual exploitation. In that case, the accused men recruited nine women from cities all over the Philippines and kept them in a boarding house in Cagayan de Oro City to engage in cybersex activities. The women were forced to establish online communication with paying clients, for a salary of PHP 15,000 per month. The clients would make specific requests from the victims that included but were not limited to baring their breasts, engaging in sexy dancing and using toys and dildos that were sent by clients to the

---

[45] Rep. Act No. 10364 (2012), § 3(a). Expanded Anti-Trafficking in Persons Act of 2012. (Emphasis and underscoring supplied.)

[46] Crim. Case No. 2009-227, May 6, 2011, decided by the Regional Trial Court (RTC) of Misamis Oriental, Branch 41.

Philippines via courier services. The court declared that even if the women were paid for their services, the act of forcing them to engage in sexual activities online was a form of sex trafficking and exploitation.

The next question is, what is cybersex? The Cybercrime Prevention Act of 2012, punishes cybersex[47] as a content related offense in Section 4(c)(1). Cybersex is distinct from the definition of trafficking in persons, because of the explicit reference to the aid of a computer system. The elements are: (1) The willful engagement, maintenance, control, or operation, directly or indirectly, (2) of any lascivious exhibition of sexual organs or sexual activity, (3) with the aid of a computer system, (4) for favor or consideration.

The law today is clear, coerced cybersex for favor or consideration is prohibited. When the regional trial court ("RTC") decision in *Solemo* was rendered on May 6, 2011, the state of the law was not as explicit, which led the accused to raise the defense of *nullum crimen, nulla poena sine lege*—in the absence of any legal prohibition, an act cannot be considered a crime.[48] In deciding the case, Judge Acebido stated that there was no specific crime denominated as cybersex, and "cybersex is just a form of pornography" notwithstanding this, he declared that exploitation was present. The accused were convicted of qualified trafficking in persons punishable by Section 4(a), and 4(e)[49] of R.A. No. 9208, the forerunner of the Expanded Anti-Trafficking in Persons Act.

What is child pornography? The Cybercrime Prevention Act of 2012 punishes child pornography as a content related offense under Section 4(c)(2), which refers to the definition in R.A. No. 9208. Section 3(b) and (c) of R.A. No. 9775, define child pornography and explicit sexual activity as follows:

> (b) "Child pornography" refers to any representation, whether visual, audio, or written combination thereof by electronic,

---

[47] *See* H. No. 1444, 15th Cong., 1st Sess. (2010), § 5 (cybersex is "any form of interactive prostitution and other forms of obscenity through the cyberspace as the primary channel"); S. No. 1879, 15th Cong., 1st Sess. (2010), § 3 ("a special form of prostitution that is conducted via the internet and the use of web cameras, by inviting people either here or in other countries to watch women, child, or men perform sexual acts in exchange for a fee paid via credit cards or other means.")

[48] Villareal v. People, G.R. No. 151258, 664 SCRA 519, Feb. 1, 2012.

[49] Rep. Act. No. 9208 (2003), § 4(a) ("To recruit, transport, transfer, harbor, provide, or receive a person by any means, including those done under the pretext of domestic or overseas employment or training or apprenticeship, for the purpose of prostitution, pornography, sexual exploitation, forced labor, slavery, involuntary servitude or debt bondage"); § 4(e) ("To maintain or hire a person to engage in prostitution or pornography.")

> mechanical, digital, optical, magnetic or any other means, of child engaged or involved in real or simulated explicit sexual activities.[50]
>
> (c) "Explicit Sexual Activity" includes actual or simulated –
> (1) As to form:
> (i) sexual intercourse or lascivious act including, but not limited to, contact involving genital to genital, oral to genital, anal to genital, or oral to anal, whether between persons of the same or opposite sex;
> (2) bestiality;
> (3) masturbation;
> (4) sadistic or masochistic abuse;
> (5) lascivious exhibition of the genitals, buttocks, breasts, pubic area and/or anus; or
> (6) use of any object or instrument for lascivious acts."[51]

For liability to attach, does the entire commercial sex act or porn production need to be completed? No, it does not. Under our present laws even attempted trafficking in persons is prohibited.[52] The current laws also address the extent of liability of principals, accomplices, and accessories. Persons who hire, recruit, or even make an offer to the victims, relatives, or parents of the victims are liable for the crime. Those who transport the victims to and from the cybersex dens, or who maintain them in dens or in the sleeping quarters will also be held responsible.[53] For example, in *Solemo,* Aminoding Rangaig was convicted for qualified trafficking in persons even if he just acted as a security guard and was not directly involved with the operations in the cybersex den. Accomplices who aid, abet or cooperate in the production of pornographic materials will also face conviction.[54] The parents who profit or assist the offender by offering their home as a location for the shooting of the video, or the chat session will also be liable.[55]

E. Problems in prosecuting cybersex

1. Problems on Jurisdiction and Evidence

Assuming jurisdiction over the accused is one of the most challenging aspects of prosecuting internet-facilitated sex trafficking. The consummation

---

[50] Rep. Act. No. 9775 (2009), § 3(b).
[51] § 3(c).
[52] Rep. Act. No.10364 (2013), § 4(a).
[53] §§ 4(k) – 4(k)(2), 4(*l*).
[54] § 4(b).
[55] § 4(c)(a).

of a single transaction can occur in two jurisdictions, making the investigation, collection of evidence, and prosecution a colossal task.[56] In this case, the victims are Filipino citizens, and the effects of the crimes are felt within the country despite the fact that the offenders never gain actual physical presence on Philippine soil.

First, letters rogatory are restricted in nature, time-consuming, transmitted through diplomatic channels and based only on comity. Second, the Philippines is a party to only nine bilateral MLATs, and one multilateral MLAT. However, the MLATs, particularly those with Australia and Hong Kong, have an exclusive list of offenses that exclude offenses of a sexual nature. Third, with respect to extradition treaties, the Philippines has yet to accede to the Budapest Convention and has extradition treaties with only 6% of countries in the world. In treaties that adopt a listing approach, cybersex is not among those enumerated crimes. Moreover, for other treaties, the dual criminality requirement is applicable. Dual criminality means that the state will cooperate only if the particular crime is penalized in both the requesting state and the requested state. For sex trafficking, cybersex in particular must be criminalized in both jurisdictions in order for the treaty to be applicable. Finally, the present formulation of the Expanded Anti-Trafficking in Persons Act on Extra-Territorial Jurisdiction [57] disregards the principle of dual criminality, and excludes cybersex from the ambit of its provisions since cybersex cannot be considered a continuing crime.

2. Problems in Evidence

Notwithstanding the fact that the Philippines is a top ten source country in the world for cybersex, and the passage of 21 years since the internet first became available in the country, our laws on the matter are relatively new and untested, and Philippine jurisprudence on electronic evidence is still largely undeveloped.

First, in *Ang v. Court of Appeals*,[58] the court made pronouncements contrary to its earlier rulings and resolutions on the applicability of the REE to all civil actions and proceedings, as well as quasi-judicial and administrative cases and criminal cases.[59] It is now unclear whether the Rules on Electronic Evidence ("REE") can be applied to criminal proceedings.

---

[56] Adel Azzam Saqf Al Hait, *Jurisdiction in Cybercrimes: A Comparative Study*, 22 J.L. POL'Y & GLOBALIZATION 75 (2014).

[57] Rep. Act No. 10364 (2013), § 26(a).

[58] Ang v. CA, G.R. No. 182835, 618 SCRA 592, Apr. 20, 2010.

[59] A.M. No. 01-7-01-SC.

Second, the author reviewed all decided cases from 1999 to 2014, and electronic evidence was only discussed in 42 of them. In several cases, particularly regarding emails, the REE discussion was obiter dictum. The last case that definitely discussed email was in 1999 or even before the passage of the E-Commerce Act and the REE. Most notably, 'Facebook' was discussed only in two cases: the 2014 case involving the graduation scandal in St. Theresa's College[60] and the case questioning the Constitutionality of the Cybercrime Prevention.[61] A search of the keyword 'Chat room' led to the same 2014 case of *Disini.*

Third, even law enforcement authorities who are supposed to be at the forefront of these procedural laws have a mistaken assumption of how the rules should be applied. The prosecution in the Priority Development Assistance Fund (PDAF) case against Senator Bong Revilla tapped NBI digital forensic investigator, Joey Narcisco, to be their expert witness.[62] Narcisco presented the prosecution with a soft copy of documents that he analyzed, the documents consisted of twenty thousand pages. The prosecution refused to present the evidence unless Narcisco printed a hard copy of every single page and affixed his signature on each and every one. This was unnecessary, and took two weeks for him to finish. Later, the evidence was not even presented in court. If the prosecutors were aware of the procedural rules in REE, they would have learned that hard copies with signature were unwarranted, and a waste of resources.

III. Acquiring Jurisdiction Over Offenders

The Philippines is one of the top ten global suppliers for the online trade of flesh,[63] thus the country should be at the forefront of the fight to ensure that its laws remain relevant, lest perpetrators escape by exploiting gaps in our procedural laws.[64]

To illustrate the complexity of crimes occurring in two jurisdictions, if a person located in the Philippines logs on to http://www.otonanojikan.com, only a registration form for recruitment of chat ladies will appear. In contrast, if a person located in Japan were to log on to the same site, he/she

---

[60] Vivares v. St. Theresa's College, G.R. No. 202666, 737 SCRA 92, Sept. 29, 2014.

[61] *Disini,* 716 SCRA 237.

[62] *Supra* note 25.

[63] Sosa, *supra* note 9.

[64] Susan W. Brenner, *Cybercrime Investigation and Prosecution: The Role of Penal and Procedural Law,* 8 MURDOCH U. ELECTRONIC J. L. 58 (2001).

would be presented with a chat room with a choice of different chat partners from the Philippines with various payment options depending on the sexual services requested.[65] In this case, the victims are the Filipino women who are forced to log on to the site and provide the services. The effects are felt within Philippine territory and in violation of Philippine laws, however the service is made available only in foreign soil.

Among the legal issues that arise in internet-facilitated sex trafficking cases are the following: If both countries file charges against the perpetrator, which state will be given priority? Which state will be permitted to exercise jurisdiction? What is the proper basis to claim jurisdiction over an act - the nationality of the offender or of the victim, the country of residence of the perpetrator, or the territory where the crime was committed?[66] What happens if there is no extradition treaty between states? If internet-facilitated sex trafficking is not listed in the treaty, or is not considered a crime in the other state, can the Philippines still acquire jurisdiction?

In answering these issues, there must be a discussion on the different theories on criminal jurisdiction relevant to internet-facilitated sex trafficking namely: (1) Territorial criminal jurisdiction; (2) Nationality principle; (3) and the Passive personality principle. This is supplemented by a discussion on international cooperation in criminal matters or the way that states gain and exchange information and evidence, and acquire jurisdiction through the following means: 1. Letters rogatory; 2. MLATs; and 3. Extradition treaties.

A. Theories of criminal jurisdiction in internet-facilitated sex trafficking

Jurisdiction is the power of a state under international law to govern persons, property and circumstances in its territory, by its municipal law.[67] State jurisdiction includes both prescriptive jurisdiction and enforcement jurisdiction. Prescriptive jurisdiction is the power to prescribe rules, whereas enforcement jurisdiction is the power to apply and enforce the rules through executive or judicial administration.[68] Prescriptive jurisdiction includes arrest, evidence gathering and incarceration.[69]

---

[65] Interview with Police Senior Inspector Allan Cabanlong, Chief, Web Services and Cybersecurity Division of the Philippine National Police (Jan. 14, 2014).

[66] Al Hait, *supra* note 56.

[67] ANTHONY AUST, HANDBOOK OF INTERNATIONAL LAW 43 (2005).

[68] MALCOLM N. SHAW, INTERNATIONAL LAW 645-646 (2008).

[69] ILIAS BANTEKOS & SUSAN NASH, INTERNATIONAL CRIMINAL LAW 71 (2007).

For the purposes of internet-facilitated sex trafficking, three relevant principles of jurisdiction–territorial, active personality (*i.e.* nationality), and passive personality (*i.e.* effects doctrine)–are discussed below. The principle of universality, and the protective principle[70] are excluded from the discussion since they are not directly related to sex trafficking, and are customarily applied to cases affecting national security, grave breaches of humanitarian law and crimes against humanity.[71]

1. Territorial Criminal Jurisdiction

Territorial Criminal Jurisdiction is the general rule in international law on account of the state's sovereignty over its national territory.[72] According to this principle, a state can exercise criminal jurisdiction if the crime or any of the elements of the crime occur within its territory,[73] even if the offenders are foreign citizens.[74] In the *Rome Labs* case,[75] the basis for jurisdiction was the territory where the acts occurred, or the hacker's location. The accused was a resident of the United Kingdom and was prosecuted for violation of Britain's Computer Misuse Act of 1990. He hacked into the Rome Labs Network located in New York and stole classified information of the artificial intelligence program of the United States Air Force.[76] Although the hacked computer system was located in the US, the UK courts assumed jurisdiction since both the accused and the computer system used to commit the crime were physically situated in the UK. UK procedural law was applied in governing the rules on search and seizure. In *Libman v. R*,[77] the Canadian Supreme Court exercised jurisdiction since the perpetration of the largest part of the fraud was in Canada, although the victims were situated in the US, and the money was sent through Central America.

---

[70] Attorney General of the Government of Israel v. Eichmann, 36 ILR 5 (1961); Re. Van de Plas, 22 ILR 205 (France, Ct. of Cassation) (1955).

[71] BANTEKOS & NASH, *supra* note 69, at 85, 83; *See also* Christopher Joyner, *Arresting Impunity: The Case For Universal Jurisdiction in Bringing War Criminals to Accountability*, 59 LAW & CONTEMP. PROBS. 153 (1996).

[72] BANTEKOS & NASH, *supra* note 69, at 73.

[73] JORGE R. COQUIA & ELIZABETH AGUILING-PANGALANGAN, CONFLICT OF LAWS: CASES, MATERIALS AND COMMENTS 49 (2000); The S.S. "Lotus" (France v. Turkey), PCIJ, Series A, No. 10 (1927).

[74] Holmes v. Bangladesh Binani Corp., 1 AC 1112; 87 ILR 365 (1989).

[75] *Cited in* Susan W. Brenner & Joseph J. Schwerha IV, *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO. L. 347 (2002).

[76] SUSAN W. BRENNER, CYBERCRIME AND THE LAW: CHALLENGES, ISSUES AND OUTCOMES 176-178 (2012).

[77] *Libman v. R.*, 21 DLR 174 200 (1986).

In the context of internet-facilitated sex trafficking - issues of jurisdiction are relatively straightforward if the operators of the dens, the pimps, or the clients are in Philippine soil. This makes the entire process of gathering evidence and witnesses more expedient. As a general rule, the Philippines follows the Principle of Territoriality.[78] The 2011 case of *People v. Solemo*[79] was the first victory against foreign-operated cybersex dens in the Philippines. The accused included two Swedish nationals, and although they were foreigners holding Swedish passports, the fact that they operated and managed the cybersex den in violation of R.A. No. 9208 merited the penalty of life imprisonment in Philippine jails and a fine of two million pesos each. As eloquently put by the court, to wit: "Foreign nationals should not abuse the hospitality and protection accorded to them during their temporary stay in the country by making it a haven for their criminal activities."

Other recent examples in the Philippine setting include the warrants issued in 2013 for the arrest of Dutch national Bartel Simon Eenkhoorn[80] and Australian national Drew Shobbrook.[81] Both were accused of operating cybersex dens in Bacolod City and Cebu City, respectively.

2. Nationality Principle (i.e. Active Personality Principle)

Under the Active Personality Principle, the nationality of the offender is the basis for the exercise of jurisdiction.[82] A state can legislate and control the activities of its nationals, even if they have relocated abroad[83] as long as there is a genuine connection of existence, interests, and sentiments.[84] Certain activities of nationals committed abroad may be prosecuted at home through extradition treaties or MLATs with the other state.[85] Theoretically, in *Solemo*[86], the Swedish government could have requested for custody over its nationals for the act, and prosecuted them under Swedish penal law.

---

[78] REV. PEN. CODE, art. 2.

[79] Crim. Case No. 2009-227, May 6, 2011, decided by RTC Misamis Oriental, Br. 41.

[80] Danny Dangcalan, *In Cybersex Den: Dutchman Nabbed, 8 Women Rescued*, The Freeman, Aug. 9, 2013, *available at* http://www.philstar.com/region/2013/08/09/1070351/cybersex-den-dutchman-nabbed-8-women-rescued.

[81] Kevin Laguna, *Cybersex Apartments in Cebu Raided*, Sun Star Cebu, Apr. 18, 2013, http://www.sunstar.com.ph/cebu/local-news/2013/04/18/cybersex-apartments-cebu-raided-278112.

[82] BANTEKOS & NASH, *supra* note 69, at 79.

[83] AUST, *supra* note 67, at 44-45.

[84] Liechtenstein v. Guatemala, 1955 ICJ 4, 23.

[85] AUST, *supra* note 67, at 45.

[86] Crim. Case No. 2009-227, May 6, 2011, decided by RTC Misamis Oriental, Br. 41.

Two other cases illustrate this principle. In both cases, the acts were consummated abroad. However, the U.S. courts exercised jurisdiction, and prosecuted the offenders on the basis of their nationality. In *Pavulak*,[87] it is interesting to note that the U.S. jury was referred to two provisions of Philippine law in the Revised Penal Code: Rape (Art. 266-A), and Corruption of minors (Art. 340).

In *United States v. Mathias*[88] the offender exchanged hundreds of emails with the mother of two minor daughters, he travelled to the Philippines to engage in sexual conduct with them. When he returned to the Philippines a second time, he was detained by Philippine authorities and advised not to leave the country pending further investigation. Notwithstanding the detention, he was able to leave the country and returned to the U.S. where he was arrested and prosecuted for violation of U.S. laws for offering to buy children for the purpose of pornography and traveling interstate to have sex with minors.[89]

3. Passive Personality Principle (i.e. the Effects Doctrine) and Rep. Act. No. 10364

In contrast to the Active Personality Principle where the basis is the nationality of the offender, in the Effects Doctrine the nationality of the victim is the foundation for the exercise of jurisdiction.[90]

In *United States v. Benitez*[91] the accused, a Columbian, raised the defense that the U.S. had no jurisdiction to try his case because the acts for which he was being prosecuted all occurred in Columbia. On appeal, the court upheld the jurisdiction of the lower court on the basis of the Passive Personality Principle. He was convicted for assault of a U.S. Drug Enforcement Agency (DEA) officer, attempted murder and theft of a U.S. government passport and DEA credentials.

In *United States v. Yunis*[92] the accused was a Lebanese man, convicted of aircraft piracy, hostage-taking and conspiracy. A group hijacked a Jordanian passenger aircraft in Lebanon, took control of the cockpit and held the civilian passengers, including two American citizens, hostage. The appellate court

---

[87] 672 F.Supp.2d 622 (D. Del. 2009), *cited in* Ibrahim et al., *supra* note 17.

[88] No.09-cr-60292 (S.D. Fla. 2010), *cited in* Ibrahim et al., *supra* note 17.

[89] Ibrahim et al., *supra* note 17.

[90] SHAW, *supra* note 68, at 664; *See* J.B. Moore, Digest of International Law 228-42 (1908).

[91] 741 F.2d 1312, 1316 (11th Cir. 1984).

[92] 924 F.2d 1086 (D.C. Cir. 1991).

affirmed the exercise of jurisdiction on the basis of both the universal principle and the passive personality principle. In so holding, the court expressly stated that "the state may punish non-nationals for crimes committed against its nationals outside of its territory, at least where the state has a particularly strong interest in the crime."[93] This incident let to the enactment of the Omnibus Diplomatic Security and Anti-Terrorism Act 1986, which grants the U.S. jurisdiction over persons charged with extra-territorial murder of U.S. nationals. Similar provisions on extra-territorial application[94] are found in The UK Taking of Hostages Act of 1982,[95] and the French Code of Penal Procedure[96]

Accordingly, a Philippine court can exercise jurisdiction over a crime committed abroad by nationals of other states, if the victims are Filipino nationals. The author conducted a survey of Philippine jurisprudence, but there has been no instance where the court has had the occasion to apply the Effects Doctrine. This is unfortunate, especially since this is a strong basis for a jurisdictional claim for a 'source country' such as the Philippines, and should be actively invoked by the government.

B. International cooperation in criminal matters

In prosecuting internet-facilitated sex trafficking, international cooperation is paramount for the transfer of investigative data, cooperation in the surveillance and the collection of evidence, and extradition of individuals.[97] Generally, international co-operation in criminal matters is done through (1) letters rogatory; (2) MLATs; and (3) extradition treaties.

---

[93] United States v. Yunis, 924 F.2d 1086 (D.C. Cir. 1991).

[94] Bantekos & Nash, *supra* note 69, at 82.

[95] An Act to Implement the International Convention Against The Taking of Hostages and For Connected Purposes, [*UK Taking of Hostages Act 1982*] (1982); *See* Definition of Hostage-taking § (1) "**A person, whatever his nationality,** who, in the United Kingdom or elsewhere (a) detains any other person ("the hostage"), and (b) in order to compel a State, international governmental organisation or person to do or abstain from doing any act, threatens to kill, injure or continue to detain the hostage, commits an offence. (2) A person guilty of an offence under this Act shall be liable, on conviction on indictment, to imprisonment for life. (Emphasis and underscoring supplied.)

[96] French Code of Criminal Procedure Code (2000) – *See* § 689 (1) "Pursuant to the international conventions referred to below, any person who renders himself guilty outside the territory of the Republic of any of the offences set out in those articles may, if in France, be prosecuted and tried by French courts."

[97] Gus Hosein, *International Co-operation as a Promise and a Threat, in* Cybercrime and Jurisdiction: A Global Survey 34 (2006).

1. Letters Rogatory

Letters rogatory are one of the oldest means of seeking formal assistance in criminal matters, and is founded on the comity of nations.[98] Comity as defined in the case of *Hilton v. Guyot*[99] is neither a matter of absolute obligation nor of mere good will or courtesy. It is the recognition that a state allows within its territory the legislative, executive and judicial acts of another country.[100] Letters rogatory are discussed in Rule 23 of the Rules on Civil Procedure on depositions pending action, *viz.*:

> "Section 12. *Commission or letters rogatory.* — A commission or letters rogatory shall be issued only when necessary or convenient, on application and notice, and on such terms, and with such direction as are just and appropriate. Officers may be designated in notices or commissions either by name or descriptive title and letters rogatory may be addressed to the appropriate judicial authority in the foreign country."[101]

Letters rogatory may be issued by a Philippine judge, on behalf of the prosecutor. It requests a judge in another jurisdiction to gather evidence for a case. The drawback to using this mode is that its scope is restricted in nature (limited to service of documents or obtaining documents from a witness), time-consuming and is transmitted through diplomatic channels.[102] Finally, since letters rogatory are based on comity, there is no assurance that the other party will assist or provide the requested information.

2. Mutual Legal Assistance Treaties (MLATs)

MLATs are applied by states in the absence of treaties or executive agreements dealing with a specific crime. MLATs are a useful tool in gaining information, sharing evidence in the investigation, and prosecuting criminal offences. Unlike letters rogatory, MLATs are based on reciprocal obligations between both states and not on mere comity. To the author, the existence of this binding obligation is the most significant distinction between MLATs and letters rogatory since it streamlines the entire process and expedites the

---

[98] ASIAN DEVELOPMENT BANK, MUTUAL LEGAL ASSISTANCE, EXTRADITION AND RECOVERY OF PROCEEDS OF CORRUPTION, ADB/OECD ANTI-CORRUPTION INITIATIVE FOR ASIA AND THE PACIFIC 35 (2007).

[99] 159 U.S. 113 (1895).

[100] COQUIA & PANGALANGAN, *supra* note 73, at 7.

[101] RULES OF COURT, Rule 23, § 12.

[102] ASIAN DEVELOPMENT BANK, *supra* note 98, at 34.

procedure. Moreover, MLATs usually contain the procedural steps and are less cumbersome than letters rogatory that are exchanged through diplomatic channels. Lastly, MLATs can include measures that will permit the state to obtain evidence in a format that is specific to the evidentiary rules of the state requesting state.[103] Note, however, that the MLAT treaties to which the Philippines is a party either expressly exclude extradition, or permit extradition only if the person and the central authority of both states agree.

The most recent case where an MLAT treaty was invoked was in the case of Mary Jane Veloso. Secretary of Justice De Lima stated that the DOJ wrote to the Indonesian Attorney General and the Minister for Justice to obtain more statements, information and testimony from Mary Jane based on the ASEAN MLAT. De Lima noted that the MLAT was instrumental in the grant of the reprieve.[104]

The US-Philippines MLAT was successfully used in 2010. The U.S. granted the request by the Office of the Ombudsman to return to the Philippine government the one hundred thousand dollars ($100,000) seized from the sons of former military comptroller Carlos Garcia.[105]

In 2012, the Philippines invoked the MLAT with Malaysia in an attempt to acquire jurisdiction over Manuel Amalilio, the founder of Amman Futures Group responsible for a "ponzi" scheme in the Philippines. Amalilio fled to Kota Kinabalu, Malaysia to evade the syndicated estafa probe. Initially, Malaysia indicated that it would cooperate and extradite Amalilio, however, it later withdrew its consent.[106]

---

[103] See statement of Mark M. Richard, Deputy Assistant Attorney General, Criminal Division, in Worldwide Review of Status of U.S. Extradition Treaties and Mutual Legal Assistance Treaties: Hearings Before the House Committee on Foreign Affairs, 100th Cong., 1st Sess. 36-37 (1987).

[104] Brian Manglungsod, *De Lima: ASEAN MLAT Helped Grant Mary Jane's Reprieve*, Interaksyon.com, Apr. 29, 2014, *at* http://www.interaksyon.com/article/109662/de-lima-asean-mutual-legal-assistance-treaty-helped-clinch-mary-janes-reprieve.

[105] Jaime Sinapit, *U.S. Returns $100,00 of Garcia's 'ill-gotten' Wealth*, INTERAKSYON.COM, Jan. 12, 2012, *at* http://www.interaksyon.com/article/21777/us-returns-100000-of-garcias-ill-gotten-wealth.

[106] Joel San Juan, *DOJ exploring options to bring Amalilio back*, BUSINESSMIRROR WEBSITE, Oct. 22, 2014, *available at* http://www.businessmirror.com.ph/doj-exploring-options-to-bring-amalilio-back.

In May 2013, the Philippines made successful use of its MLAT with Taiwan[107] in the Balintang Channel shooting of Taiwanese fishermen. Philippine investigators travelled to Taiwan and used the information obtained to file homicide charges against eight Philippine Coast guard officials.[108]

3. Extradition Treaties

Extradition is the surrender of a person suspected, charged or convicted of a criminal offense by one state to another.[109] The right and obligation to extradite arises from treaties, however, states shall make their own determination of the validity of the request, and in no case will there be extradition for an offense not included in a treaty of extradition.[110]

i. Bilateral Extradition Treaties to which the Philippines is a State Party[111]

To date, the Philippines has signed bilateral extradition treaties with only 13 countries: Indonesia, 1976; Thailand, 1984; Switzerland, 1989; Canada, 1990; Australia, 1991; Korea, 1993; Micronesia, 1994; USA, 1996; Hong Kong, 1997; People's Republic of China, 2006; Spain, 2014; India, 2014; and United Kingdom, 2014. The Philippines can only acquire jurisdiction over nationals who have committed or are suspected of committing internet-facilitated sex trafficking from 6% of the 195 independent states in the world.[112]

This problem is heightened in cases where the country of the offender refuses to exercise jurisdiction over the case. A hypothetical example is a case where a British citizen pays for an online show performed by a 12-year old Filipino boy located in Angeles City. UK authorities may refuse to exercise jurisdiction because the offense is not significantly linked with the domestic jurisdiction as required by the Computer Misuse Act of 1990.

---

[107] Official Statement of the Taipei Economic and Cultural Office in the Philippines, June 19, 2013, *available at* http://www.roc-taiwan.org/PH/ct.asp?xItem=392849&ctNode=4695&mp=272.

[108] Mark Meruenas, *The Many Times the MLAT aided the Philippines,* GMA NEWS ONLINE, April 30, 2015, *at* http://www.gmanetwork.com/news/story/479246/news/specialreports/the-many-times-the-mutual-legal-assistance-treaty-aided-phl.

[109] Gupta, *Sanctum for the War Criminal: Extradition Law and the International Criminal Court,* 3 CAL. CRIM. L. REV. 1 (2000), *citing* Bassett More, 1 TREATISE ON EXTRADITION AND INTERSTATE RENDITION (1891); BLACK'S LAW DICTIONARY 585 (6th ed. 1990).

[110] Wright v. CA, G.R. No. 113213, 235 SCRA 341, Aug. 15, 1994.

[111] *See* Appendix C, "Philippine extradition treaties with ten states."

[112] U.S. Department of State Bureau of Intelligence and Research, Fact Sheet on Independent States of the World, *available at* http://www.state.gov/s/inr/rls/4250.htm.

The refusal to assume jurisdiction was shown in the Gary McKinnon case[113], where McKinnon, a systems administrator in the UK hacked into ninety-seven U.S. Military and NASA computers, stole passwords and deleted critical systems administration files. The UK Crown Prosecution Service did not bring any charges against him claiming that although the computer was located within the UK, "the target and the damage were transatlantic"[114] (*i.e.* an insufficient domestic link). It was only after the U.S. and the UK signed an extradition treaty that the U.S. was able to exercise jurisdiction over McKinnon and a warrant for his arrest was issued.

To the credit of the Philippine Senate, they finally concurred in the ratification of an extradition treaty with the UK in 2014. Since we are dealing with actual victims who are at risk of experiencing severe psychological and developmental problems,[115] the Philippines simply cannot wait for an actual case to arise before it signs an extradition treaty with the state of an accused perpetrator from any of the remaining 182 countries.

In the case of *Wright v. Court of Appeals*,[116] the Supreme Court made it very clear that a State cannot surrender any individual for an offense not included in a treaty of extradition. The technical terms and definitions for the crime in both states need not be identical. What is critical is the substantive underlying conduct.[117]

The Philippines adopts two approaches in extradition law: (1) the listing approach where the specific crimes for which extradition will be granted are enumerated, and (2) the dual criminality approach where extradition will be granted as long as the crime is punished in both jurisdictions.[118]

Generally, the Philippines adopts the dual criminality approach. On the other hand, the treaties with Hong Kong, Indonesia and Thailand follow a listing approach. An examination of these three treaties shows that none include the crime of internet-facilitated sex trafficking, making the treaties essentially nugatory in the prosecution of this crime.

---

[113] Al Hait, *supra* note 56, at 81.

[114] *Id.*

[115] Sigurjónsdóttir, *supra* note 21, at 8-9.

[116] *Wright*, 235 SCRA 341.

[117] ASEAN Legal Handbook on International Legal Cooperation in Trafficking in Persons Cases 120 (2010).

[118] Gana, *Extradition and Legal Experience: The Philippine Experience*, *in* UN Asia and Far East Institute for the Prevention of Crime and Treatment of Offenders Resource Material Series No. 79 50 (1999).

1. Bilateral Extradition Treaty with Indonesia

In the list of extraditable crimes, the only provision that could be applied is "unlawful sexual acts with or upon minors under the age specified in the penal laws of both countries."[119] This leaves victims who are overage without protection, and it is unclear whether the sexual acts include acts committed through the internet.

2. Bilateral Extradition Treaty with Thailand

This treaty contains a similar provision to the extradition treaty with Indonesia,[120] thus, the same problems and criticisms of the treaty with Indonesia are also applicable. The unlawful sexual acts must be committed against minors or under the age specified in the penal laws of both countries.[121]

3. Bilateral Extradition Treaty with Hong Kong

Of the three treaties that adopted the listing approach, this treaty is the most promising in the realm of cybersex since it includes offenses of a sexual nature, [122] offenses against prostitution and premises kept for prostitution.[123] However, criminal laws are construed strictly against the state and in favor of the offender, thus it remains to be seen how this provision will be construed in light of the internet.[124]

In all other cases, the Philippines adopts a dual criminality approach. This means that the crime must be recognized in both the requesting state

---

[119] Treaty on Extradition Between the Republic of the Philippines and the Republic of Indonesia (1976) [hereinafter "Extradition Treaty with Indonesia"], Art. 2(a)(2).

[120] Treaty between the Government of the Republic of the Philippines and the Government of the Kingdom of Thailand Relating to Extradition (1981) [hereinafter "Extradition Treaty with Thailand"], Art. 2(1)(B) "rape, indecent assault; unlawful sexual acts with or upon minors under the age specified by the penal laws of both Parties".

[121] *Id.*

[122] Agreement between the Government of the Republic of the Philippines and the Government of Hong Kong for the Surrender of Accused and Convicted Persons (1995) [hereinafter "Extradition Treaty with Hong Kong"], Art. 2 (vii) "offences of a sexual nature including rape, sexual assault, indecent assault, and unlawful sexual acts upon children; statutory sexual offences"; Extradition Treaty with Hong Kong, Art. 2(viii).

[123] Extradition Treaty with Hong Kong, Art. 2(ix) "offences against laws relation to prostitution and premises kept for the purposes of prostitution."

[124] Robert Cryer et al., An Introduction to International Criminal Law and Procedure 9 (2007).

and the requested state.[125] Sec. 26-A of R.A. No. 9208 on extraterritorial jurisdiction disregards this bedrock principle of dual criminality:

> SEC. 26-A. *Extra-Territorial Jurisdiction.* – The State shall exercise jurisdiction over any act defined and penalized under this Act, **even if committed outside the Philippines and whether or not such act or acts constitute an offense at the place of commission**, the crime being a continuing offense, having been commenced in the Philippines and other elements having been committed in another country, if the suspect or accused
> (a) Is a Filipino citizen; or
> (b) Is a permanent resident of the Philippines; or
> (c) Has committed the act against a citizen of the Philippines.[126]

Extradition treaties must be strictly construed, as they necessarily involve the liberty of individuals, and in many cases they involve the nationals of that state.[127] If we analyze the provisions of the extradition treaties to which the Philippines is a party, clearly no extradition request will be granted on the grounds of cybersex or pornography. The author has searched in vain for any other country in the world that criminalizes cybersex, especially between adults, even if the element of coercion is present. It is noteworthy that even the Budapest Convention excludes cybersex from the offenses listed. The Philippines cannot unilaterally declare that an act is to be included in the extraditable offenses by mere enactment of domestic legislation.

Legislators attempted to circumvent the principle of dual criminality by classifying it as a continuing crime as shown below:

> SEC. 26-A. *Extra-Territorial Jurisdiction.* – The State shall exercise jurisdiction over any act defined and penalized under this Act, even if committed outside the Philippines and whether or not such act or acts constitute an offense at the place of commission, **the crime being a continuing offense, having been commenced in the Philippines and other elements having been committed in another country**, if the suspect or accused:
> x x x
> (c) **Has committed the act against a citizen of the Philippines.**[128]

---

[125] Gana, *supra* note 118.

[126] Rep. Act No. 9208 (2003), § 26-A, *amended by* Rep. Act No. 10364 (2013). (Emphasis and underscoring supplied.)

[127] CHRISTOPHER PYLE, EXTRADITION, POLITICS AND HUMAN RIGHTS 312 (2001).

[128] Rep. Act No. 9208 (2003), § 26-A, *amended by* Rep. Act No. 10364 (2013). (Emphasis and underscoring supplied.)

The author submits that foreigners situated in other jurisdictions cannot be held liable for internet-facilitated sex trafficking if the crimes of pornography and cybersex are characterized as continuing crimes. These crimes cannot be considered continuing crimes for the simple reason that not all the acts punished by R.A. No. 10364 are commenced in the Philippines. To argue this point, the author will discuss the definition of continuing crimes, then contrast the definition to the acts punished.

First, in the case of *Mallari v. People,*[129] a continuing crime was referred to as a continuous or continued offense, it was defined as a single crime consisting of a series of acts all arising from one criminal resolution.[130] In *Gamboa v. Court of Appeals*, the court stated that the acts material and essential to the crime, and requisite to its consummation, start in one jurisdiction, and other acts occur act in another jurisdiction. [131] As can be seen, to be considered a continuing crime, the elements must occur in at least two or more jurisdictions.

Second, an examination of the statutes will show that by merely obtaining,[132] luring, grooming, [133]or hiring[134] a person to engage in sexual exploitation, or by willfully accessing,[135] or possessing[136] child pornography – the crime of sex trafficking is already consummated. Consequently, if we apply the definition of continuing crimes to these acts, prosecutors cannot attain extra-territorial jurisdiction over nationals in other countries who perform them. Prosecutors can only successfully prosecute cases where the act was literally and actually commenced in the Philippines. This severely limits the effectiveness of prosecutors. An amendment to cure this problem will be discussed in the recommendations in Part III(C).

ii. Multilateral Extradition Treaty – The Budapest Convention

The Philippines has not acceded to the Budapest Convention despite the fact that the Supreme Court recently upheld the constitutionality of the Anti-Cybercrime Prevention Act,[137] which was based on the fundamental concepts of the Budapest Convention. During the Senate deliberations on the

---

[129] Mallari v. People, G.R. No. L-58886, 168 SCRA 422, 429, Dec. 13, 1998.
[130] *Id.*
[131] Gamboa v. CA, G.R. No. L-41054, 68 SCRA 308, Nov. 28, 1975.
[132] Rep. Act No. 10364 (2013), § 4(a).
[133] Rep. Act No. 9775 (2009), § 4(h).
[134] Rep. Act No. 10364 (2013), § 4(e)
[135] Rep. Act No. 9775 (2009), § 4(j).
[136] *Id.*, § 4(*l*).
[137] *Disini,* 716 SCRA 237.

Cybercrime Prevention Bill both Senator Angara and Senator Santiago raised their concerns on the failure of the country to accede to the Convention since the cooperation of other countries is essential to the enforcement of the Bill.

The Budapest Convention entered into force in 2004. It is the first international treaty on crimes committed via the internet and contains detailed rules to harmonize rules of procedure and evidence, and to streamline mutual assistance and cooperation. Most importantly, it will enable the Philippines to exercise jurisdiction over nationals of other countries with which the Philippines has no extradition treaty but are parties to the convention. The treaty itself will substitute as the legal basis for extradition in lieu of another bilateral agreement, as provided in Art. 24(3) of the Convention.

iii. Cases where the Philippines invoked the Extradition Treaties

The author surveyed the annual reports of the DOJ, which is the central authority of the government relative to MLATs and extradition treaties, from 2002 to the latest available report in 2013.

In 2001 the DOJ started working on the extradition request to the United States for Jaime Dichaves.[138] Dichaves was tagged as one of the alleged corporate owners of the Estrada Mansions. It also sent extradition requests for Charlie "Atong" Ang and Yolanda Ricaforte.[139] Ang was extradited to the country in November 2006.[140]

In 2003 the DOJ report stated that the legal staff extradited four persons from the country to the United States, and handled two cases of extradition from the Philippines involving two persons. The persons were unnamed in the report.[141]

Angelito Alix was extradited from the United States to the Philippines in 2007. He was charged with estafa before the Pasig RTC.[142] In 2008, the Taskforce Against Political Violence initiated the extradition of accused in the Dacer-Corbito double murder case.[143]

---

[138] 2001-2002 DOJ Annual Report, p. 9.

[139] *Id.*

[140] Reynaldo Santos Jr. and Michael Bueza, *Cast in Erap Plunder Case: Where are they now?*, RAPPLER, April 24, 2014, *at* www.rappler.com/newsbreak/investigative/56022-cast-erap-plunder-case.

[141] 2003 DOJ Annual Report, p. 3.

[142] 2007 DOJ Annual Report, p. 23.

[143] 2008 DOJ Annual Report, p. 9.

2009 was a banner year for the DOJ. Three fugitives were extradited to the United States – PNP officers Cezar Mancao II and Glenn Dumlao for the double murder of publicist Salvador Dacer and his driver Emmanuel Corbito; and Madhatta Amir Haipe a suspected member of the Abu Sayyaf Group. Juan "Paco" Larranaga was extradited to Spain in order to continue the service of his sentence for the rape-slay of the Chiong sisters.[144]

From the above reports, it is clear that extradition is a viable option to curb internet-facilitated sex trafficking. In fact, there has been a rise in the invocation of the treaties in recent years.

C. Synthesis, analysis, and recommendations

To date, Philippine authorities have targeted their efforts on the supply side of the crime by focusing on sex traffickers and conducting raids in alleged cybersex shops. Despite the bold efforts of law enforcement agencies, cybersex is still performed in 38% of the provinces in the country and the Philippines is a top ten source country in the world. This leads to the inescapable conclusion that the government should take more aggressive and active steps in enforcement. Granted that other countries and international organizations are targeting and prosecuting cybersex predators, the Philippines cannot simply rely on their efforts or their judicial systems alone. Moreover, there is no guarantee that these countries will be able to effectively prosecute all cases involving Filipino women, children and cybersex performers. The author proposes that the government adopt a shift in its policy, and focus on the perpetrators themselves, or the source of demand. In line with this, the author of the paper makes the following recommendations.

With respect to treaty law, first, the Philippines should accede to the Budapest Convention. Second, the country should enter into more MLATs and bilateral extradition treaties with other states. Third, it should seek to expand the scope of the list of crimes included in the ambit of the treaties to include cybersex trafficking and crimes of a sexual nature.

1. The Philippines should accede to the Budapest Convention

Acceding to the Budapest Convention will speed up the process of acquiring jurisdiction because the accession and ratification of this single treaty will obviate the need to incorporate multiple bilateral extradition treaties into Philippine law. Art. 42 of the Convention authorizes states parties to make reservations to the treaty which will modify the obligations of the

[144] 2009 DOJ Annual Report, p. 6.

reserving state vis-à-vis other parties.[145] Contentious provisions such as the expedited preservation of stored computer data, [146] or the expedited preservation and partial disclosure[147] of other computer data, and other controversial articles may be excluded to the extent that the reservations are not contrary to the object and purpose of the Budapest Convention.[148]

Moreover, the concerns raised by the petitioners in *Disini* and the provisions struck down by the Supreme Court as unconstitutional are not among the provisions that are excluded from reservations as enumerated in Sec. 42 of the Convention.

2. The Philippines should enter into more MLATs and bilateral extradition treaties with other states.

Even if the Philippines acceded and ratified the Budapest Convention, not all states are parties to the convention and there is no guarantee that other states will sign and ratify it.

This leads to the second recommendation with respect to treaty law: The Philippines should continue to strengthen its diplomatic relations with other countries and enter into more MLATs and bilateral extradition treaties to ensure that prosecutors can acquire jurisdiction over accused individuals from other states. By no stretch of the imagination can the existing extradition treaties with 6%, and MLATs with 35%, of the 195 independent states in the world[149] give our Filipino men, women and children, effective protection in our fight against internet-facilitated sex trafficking.

i. MLATs to which the Philippines is a State Party

As of this writing, the Philippines has concluded nine bilateral MLATs with other states and one multilateral MLAT–the 2004 ASEAN Treaty on MLA in Criminal Matters. Assistance on criminal matters, which may include cybersex operations, can be obtained under the U.S., Korea, Spain, Switzerland, China, the UK, and ASEAN MLATs. As regards the treaties with Australia and Hong Kong, however, the list of crimes is specific and excludes crimes of a sexual nature. Extradition and transfer of custody

---

[145] Vienna Convention on the Law of Treaties art. 21(1), May 23, 1969, 1155 U.N.T.S. 331 [hereinafter "VCLOT"], art. 21 (1).

[146] Council of Europe, Convention on Cybercrime (2001), art. 16.

[147] *Id.*, art. 17.

[148] VCLOT, art. 19(c).

[149] *Supra* note 112.

through an MLAT (either unilaterally or based on the consent of both the party and the requested state) can be had with the U.S., Hong Kong, Spain and the UK. There is no such concept in our MLAT treaties with Australia, Korea, Spain, China and ASEAN.[150]

As previously discussed, the Philippine experience has shown that the use of MLATs, when properly invoked, can be effective. In order to make them even more effective, the Philippines should endeavor to expand the list of crimes in the MLATs with Australia and Hong Kong to include sex trafficking, and crimes of a sexual nature. At present, the list of crimes under both treaties are exclusive, thus no information or evidence can be obtained regarding internet-facilitated sex trafficking. Additionally, for the countries with which the Philippines has existing MLATs, it should endeavor to make more active use of the communication and legal channels.

ii. Bilateral Extradition Treaties

Similar to MLATs, extradition treaties have been successfully used by the Philippines based on the DOJ annual reports from 2001 to 2013. Nine persons were extradited to the Philippines, and six persons were extradited abroad based on requests received from other states.

The author analyzed the thirteen bilateral extradition treaties to which the Philippines is a party and noted two problems. First, majority of the countries adopted a dual criminality approach, which means that the crime (cybersex) must be penalized in both the requesting state and the requested state. This requirement was included in the treaties with China, Korea, USA, Australia, Canada, Thailand, Indonesia, Switzerland, and the UK. It is noteworthy to reiterate the need to revisit the definition of cybersex in R.A. No. 10175 because the offense of cybersex is not included in the Budapest Convention, which is the basis for the Anti-Cybercrime law.[151]

Second, the bilateral treaties that include sexual offenses are limited to minor victims. This leaves overage victims without any protection. We see this in the treaties with Indonesia and Thailand.[152] To further compound the problems, it is unclear whether the sexual acts can be construed to include acts committed through the internet as there are no decided cases as of yet.

---

[150] *See* Appendix B, "Philippine MLATs with eight states, the ASEAN MLAT and selected provisions."

[151] *Gonzales*, 137 SCRA 717.

[152] Extradition Treaty with Indonesia (1976), art. 2(a)(2); Extradition Treaty with Thailand (1981), art. 2(1)(B).

Consequently, the author recommends that, first, the Philippines should enter into negotiations to amend these bilateral treaties to include the crimes of cybersex and sexual offenses; second, it should negotiate to extend the coverage of the sexual offenses to give protection not just to minors but to women and men of legal age who are victims of sexual exploitation; and third, it should enter into agreements to supplement the treaties in cases where the other state refuses to amend the existing treaty.

3. The Philippines should amend current law to resolve the issues on dual criminality and continuing crimes

In the realm of Philippine statutes, the author respectfully submits the following recommendations to amend Sec. 26-A of R.A. No. 9208, as amended by R.A. No. 10364, on extra-territorial jurisdiction to remedy the noted problems on dual criminality and continuing crimes. Together, the combined proposals are reflective of the international treaties to which the Philippines is a party, and expands the scope and reach of the government for extra-territorial jurisdiction. The current provision reads as follows:

> SEC. 26-A. *Extra-Territorial Jurisdiction.* – The State shall exercise jurisdiction over any act defined and penalized under this Act, even if committed outside the Philippines and **whether or not such act or acts constitute an offense at the place of commission**, the crime being a continuing offense, having been commenced in the Philippines and other elements having been committed in another country, if the suspect or accused:
> (a) Is a Filipino citizen; or
> (b) Is a permanent resident of the Philippines; or
> (c) Has committed the act against a citizen of the Philippines.
>
> No prosecution may be commenced against a person under this section if a foreign government, in accordance with jurisdiction recognized by the Philippines, has prosecuted or is prosecuting such person for the conduct constituting such offense, except upon the approval of the Secretary of Justice.
>
> The government may surrender or extradite persons accused of trafficking in the Philippines to the appropriate international court if any, or to another State pursuant to the applicable extradition laws and treaties.[153]

---

[153] Rep. Act No. 9208 (2003), § 26-A, *amended by* Rep. Act No. 10364 (2013). (Emphasis and underscoring supplied.)

With respect to dual criminality, the author proposes that the first paragraph of the provision be amended, to read:

> The State shall exercise jurisdiction over any act defined and penalized under this Act even if committed outside the Philippines, *provided that the conduct is punished by the laws of the requested state or any bilateral or multilateral treaties to which the requested state is a party.*[154]

To resolve the problems on continuing crimes, the author proposes that the following clause be inserted after paragraph (c):

> *If the felony is not a continuing offense, having been committed in another country, but the act is committed against a citizen of the Philippines, the state may exercise jurisdiction under the applicable basis of international law.*

Thus, combined with the earlier recommendation to address dual criminality, the entire proposed amendment should read as follows:

> SEC. 26-A. *Extra-Territorial Jurisdiction.* - The state shall exercise jurisdiction over any act defined and penalized under this Act even if committed outside the Philippines, **provided that the conduct is punished by the laws of the requested state or any bilateral or multilateral treaties to which the requested state is a party**. If the felony is a continuing offense, having been commenced in the Philippines and other elements having been committed in another country, the state shall exercise jurisdiction over the act if the suspect or accused:
> (a) Is a Filipino citizen; or
> (b) Is a permanent resident of the Philippines; or
> (c) Has committed the act against a citizen of the Philippines.
>
> **If the felony is not a continuing offense, having been committed in another country, but the act is committed against a citizen of the Philippines, the state may exercise jurisdiction under the applicable basis of international law**.
>
> xxx.[155]

Together, the combined proposals to amend Sec. 26-A of R.A. No. 9208, as amended by Rep. Act No. 10364 are reflective of the international treaties to which the Philippines is a party, and expand the scope and reach of the government for extraterritorial jurisdiction.

---

[154] Amended portion is italicized.

[155] Proposed amendments are highlighted and underlined.

IV. Applying the Rules on Electronic Evidence

A. Philippine statutes, implementing rules and regulations, and the Supreme Court circular on rules of electronic evidence ("REE")

The Philippines was first connected to the internet in 1994.[156] Six years lapsed before the promulgation of rules specifically addressing the use of the internet, penalties, or the admissibility, evidentiary weight and attribution of electronic evidence. The development in these rules was spurred on by the infamous "ILOVEYOUVIRUS" that was unleashed in 2000 by Onel de Guzman, a Filipino in the Pandacan neighborhood of Manila. The effects of the virus were felt in Europe, the U.S. and Asia (especially Hong Kong) with an estimated cost of up to 8.7 billion dollars in damages worldwide.[157] Despite tremendous pressure, the Philippine government was unable to bring charges against de Guzman as there were no laws criminalizing his act at the time he unleashed the virus, following the criminal law principle of *nulla crimen sine lege.*

International and domestic pressure weighed heavily on the government, in response, the E-Commerce Act (R.A. No. 8792) was signed into law on June 14, 2000. The implementing rules and regulations (IRR) were released the following month on July 14, 2000 and was signed by the then Secretaries of the Department of Trade and Industry, the Department of Budget and Management, and then Governor of the *Bangko Sentral ng Pilipinas.* The Supreme Court followed suit on July 17, 2001 when it issued the Rules on Electronic Evidence in A.M. No. 01-7-01-SC. The latest development was the Cybercrime Prevention Act of 2012 approved in September 12, 2012.

There is some confusion as to whether the REE can be applied to criminal cases, based on the latest Supreme Court ruling in 2010.[158] This is a significant departure from its earlier pronouncements.

In 2001, the Supreme Court issued a circular on the rules of electronic evidence. It declared that the REE were applicable to all civil actions

---

[156] Miguel A.L. Paraz, *Developing a Viable Framework for Commercial Internet Operations in the Asia-Pacific Region: The Philippine Experience, available at* http://www.isoc.org/inet97/proceedings/E6/E6_1.HTM.

[157] Jack L. Brock, Jr., *Critical Infrastructure Protection "ILOVEYOU" Computer Virus Highlights Need for Improved Alert and Coordination Capabilities*, 2 DTIC ONLINE INFORMATION FOR THE DEFENSE COMMUNITY (2000).

[158] *Ang*, 618 SCRA 592.

and proceedings, as well as quasi-judicial and administrative cases.[159] In 2002, the coverage was expanded to apply to criminal cases.[160] Eight year later, in April 2010, the Court speaking through the *ponencia* of Justice Abad, declared "the rules [REE] he [defendant] cites **do not apply to the present criminal action. The Rules on Electronic Evidence applies only to civil actions, quasi-judicial proceedings, and administrative proceedings.**"[161]

Significantly, the applicability of the REE to criminal cases was revoked. Following the ruling in *Ang* in prosecuting a case for internet-facilitated sex trafficking, prosecutors cannot longer make reference to the REE for authentication, and presentation of evidence.[162] The Supreme Court has not issued any clarification on the matter, and has not had the occasion to explain its intentions through a decided case. It is entirely possible, that the statement was mere dicta and the REE are still applicable to criminal cases.

B. Rules on Electronic Evidence as applied in Philippine judicial decisions

The author conducted a search of Philippine jurisprudence using the keywords 'E-Commerce Act', 'electronic evidence', 'email', 'email', 'website', 'text message', 'SMS', 'chat room' and 'Facebook'. This search led to only 42 cases, and in several of those cases, the keywords were only mentioned with no discussion of the proof given to authenticate the evidence.

Most notably, 'Facebook' was discussed only in two cases, the 2014 case involving the graduation scandal in St. Theresa's College[163] and the case questioning the Constitutionality of the Anti-Cybercrime law.[164] A search of the keyword 'chat room' led to the same 2014 case of *Disini*.

Philippine jurisprudence on electronic evidence is still largely undeveloped, and is still at its infancy state despite the passage of 21 years since the internet first became available in the country. The author prepared a summary of the decided cases regarding: facsimile/fax; photocopies; text messages (SMS) and Multimedia Message (MMS); electronic mail/email; chat room messages; Facebook posts and messages; and websites.

---

[159] A.M. No. 01-7-01-SC.

[160] Supreme Court resolution re: Expansion of the Coverage of the Rules on Electronic Evidence, dated Sept. 24, 2002.

[161] *Ang*, 618 SCRA at 604. (Emphasis supplied.)

[162] CIVIL CODE, art. 8.

[163] *Vivares*, 737 SCRA 92.

[164] *Disini*, 716 SCRA 237.

1. Facsimile/fax

Facsimiles or faxes are not admissible as electronic evidence. In *MCC Industrial Sales Corp. v. Ssangyong Corp.*[165] the petitioner was a domestic corporation engaged in the business of import and wholesale of stainless steel products. The respondent was its supplier with a head office in South Korea. The two corporations conducted business through telephone calls and facsimile or telecopy transmissions. Petitioner would send the *pro forma* invoices containing the details of the order to respondent, if the latter conforms thereto, its representative affixes his signature on the faxed copy and sends it back, again by fax. Respondent filed a civil action against petitioner for damages. Petitioner filed a demurrer to evidence alleging that the respondent failed to present the original copies of the *pro forma* invoices to prove the perfection of the alleged contract of sale. Petitioner claims that the photocopies of the pro forma invoices are inadmissible in evidence, because the E-Commerce Act only admits the original *fax* transmittal as the best evidence. Respondent contends that the original *facsimile* transmittal of the invoice is admissible in evidence because it is an electronic document.

The Supreme Court ruled that the original facsimile transmittals are inadmissible in evidence. In so ruling, the Court stated that in an ordinary facsimile transmission, there exists an original *paper-based* information or data that is scanned, sent through a phone line, and reprinted at the receiving end. The two copies are distinct from each other.

This holding was similar to the 1997 case of *Garvida v. Sales*[166] and the 2011 case of *Torres v. Philippine Amusement and Gaming Corp.*,[167] where the counsels sent their respective pleadings through facsimile. In rejecting the pleadings, the Supreme Court stated that a facsimile is not a genuine and original pleading, it is as best, an exact copy preserving all the marks of the original, and a facsimile.[168] Consequently, a facsimile transmission cannot be considered as electronic evidence. It is not the functional equivalent of an original under the Best Evidence Rule and is not admissible as electronic evidence.[169]

---

[165] G.R. No. 170633, Oct. 17, 2007.

[166] Garvida v. Sales, G.R. No. 124893, 271 SCRA 767, Apr. 18, 1997.

[167] Torres v. Philippine Amusement and Gaming Corporation, G.R. No. 193531, 269 SCRA 344, Dec. 14, 2011.

[168] *Garvida*, 271 SCRA 767.

[169] *Torres*, 269 SCRA 344.

2. Photocopies

In *National Power Corporation v. Codilla*[170] the court categorically stated that Xerox copies do not constitute the electronic evidence defined in Section 1 of Rule 2 of the REE since the information in those Xerox or photocopies was not received, recorded, retrieved or produced electronically. In this case, the vessel owned by the respondent bumped and damaged the vessel of the petitioner, who filed a complaint for damages. To prove his case, the petitioner presented photocopies of several documents. He alleged that the photocopies that were presented as documentary evidence are the functional equivalent of the original. Petitioner maintained that "an electronic document" can also refer to other modes of written expression that are produced electronically, such as photocopies, as included in the section's catch-all proviso: 'any print-out or output, readable by sight or other means.' The court rejected this reasoning, ruled in favor of the defendant's objections and granted the motion objecting to the admissibility of the documents as they did not comply with the rule on best evidence.

3. Text messages (SMS) and Multimedia Message (MMS)

The 2005 administrative case of *Nuez v. Cruz-Apao*[171] was the first case where the court had the opportunity to admit text messages as ephemeral electronic communication under Rule 2 of the REE. The respondent was an Executive Assistant II of the Acting Division Clerk of Court of the Fifteenth Division, Court of Appeals. She solicited 1 million pesos from the complainant in exchange for a speedy and favorable decision of the latter's pending case in the Court of Appeals. To support his case, complainant presented the text messages he received from the respondent. As recipient of the messages, he had personal knowledge of the contents of the SMS and could testify to their import. Moreover, according to the records of the case in the Court of Appeals, respondent signed and attested to the veracity of the text messages. It is interesting to note that during her testimony, when the respondent was asked if she had sent the text messages contained in complainant's cellphone, she only admitted to sending the messages that were not incriminating, but when asked about the messages with incriminating information regarding the transaction, she claimed she did not remember sending those messages.[172]

---

[170] G.R. No. 170491, 520 SCRA 412, Apr. 3, 2007.

[171] A.M. No. CA-05-18-P, 455 SCRA 288, Apr. 12, 2005.

[172] *Id.*

In another administrative case, *Magtolis v. Salud*,[173] the respondent was charged and held liable for offenses of inefficiency and incompetence of official duty, conduct grossly prejudicial to the best interest of the service, and directly or indirectly having a financial and material interest in an official transaction. In the affidavit of the complainant, all 23 messages, with their verbatim content and the time and date stamp were included. Justice Magtolis checked all the text messages in the cellphone of the complainant in the presence of the counsel of respondent. Justice Magtolis also gave the complainant instructions to preserve the messages until he was permitted to erase them. Through questioning, respondent admitted that the cellphone number in the affidavit was his. In his defense respondent claimed that that the admission of the text messages as evidence against him constituted a violation of his right to privacy. The court rejected this claim and classified the texts as ephemeral electronic communication, making specific reference to the earlier case of *Nuez v. Cruz-Apao*.[174]

Ownership of the cellular phone used to send the message is irrelevant, and impersonation of the sender is not a bar to admissibility of the evidence. In the homicide case of *People v. Enojas*,[175] Enojas, accidentally left his cellular phone in the abandoned taxi. The policemen found it and monitored the messages in his mobile phone and, posing as Enojas, communicated with the other accused and set an entrapment operation. The prosecution presented the transcripts of the mobile phone text messages between Enojas and some of his co-accused. The defense argued that the text messages were inadmissible, not having been properly identified. The court admitted the text messages, and ruled that the testimony of the policeman who posed as the accused Enojas, exchanged text messages with the other accused in order to identify and entrap them was admissible. As the recipient of those messages sent from and to the mobile phone in his possession, the policeman had personal knowledge of such messages and was competent to testify on them.

The affidavit used as evidence of the text message must be properly sworn to before a competent officer. Otherwise, it is inadmissible in evidence. In *Callo-Claridad v. Esteban*[176] the Court excluded from the evidence the circumstance that the victim sent a text message to his girlfriend that he was on his way to get the tires at around 7:09 P.M. of February 27, 2007 because his girlfriend's affidavit was not sworn to before a competent officer. The

---

[173] A.M. No. CA-05-20-P, 469 SCRA 439, Sept. 9, 2005.

[174] *Nuez*, 455 SCRA 288.

[175] G.R. No. 204894, 718 SCRA 313, Mar. 10, 2014.

[176] G.R. No. 191567, 694 SCRA 185, 199, Mar. 20, 2013.

Court also stated that "there was also no evidence of the alleged text message pursuant to the law on admissibility of electronic evidence" but did not expound on this point.

Ang v. Court of Appeals[177] is a case rich with doctrines for our purposes. In this case, the accused sent his former girlfriend an MMS with the picture of a naked woman with her legs spread wide open. The photo was not of the recipient, but with her face superimposed on it. Under the supervision of the police, the complainant contacted the accused and he agreed to meet her in a resort. When he arrived, the police officers intercepted and arrested him. They searched him and seized his Sony Ericsson P900 cellphone and several SIM cards. The prosecution presented an expert witness who testified on how pictures can be manipulated and enhanced by computer to make it appear that the face and the body belonged to just one person with the use of a Sony Ericsson P900 cellphone.

The accused raised two defenses in the Supreme Court: First, he claimed that the evidence presented against him should be deemed inadmissible since he was arrested and certain items were seized from him without any warrant. Second, he claimed that the obscene picture sent to his girlfriend through a text message constituted an electronic document therefore it should be authenticated by means of an electronic signature.

The Supreme Court denied his appeal. First, the prosecution did not present in evidence either the cellphone or the SIM cards that the police officers seized from him at the time of his arrest. The prosecution only presented a photograph depicting the Sony Ericsson P900 cellphone that was used, and the accused admitting to owning the cellphone in the photo. The prosecution was able to prove that the accused sent the obscene photo, because they used the number to summon him to the place where the entrapment operation occurred. Second, the right to object to the admissibility of the photo was waived, because it was raised before the Supreme Court for the first time on appeal. Third, the court speaking through Justice Abad stated that the REE that the accused was referring to on authentication was inapplicable to the present criminal action. "The Rules on Electronic Evidence applies only to civil actions, quasi-judicial proceedings, and administrative proceedings."[178]

---

[177] *Ang*, 618 SCRA 592.

[178] *Id.*

4. Electronic mail/ email

Interestingly, the only case where the Court definitively discussed email authentication was decided in 1999, or before the issuance of the E-commerce Act, its IRR and the REE.

In *IBM Philippines, Inc. v. NLRC*[179] the petitioner dismissed the respondent from work on the ground of habitual tardiness and absenteeism. To prove that the respondent was sufficiently notified of the charges, the petitioner submitted print-outs of 18 company emails wherein it gave the respondent repeated warnings. The Supreme Court found the print-outs of the emails inadmissible on two grounds: First, the computer print-outs afforded no assurance of their authenticity because they were unsigned either by the sender or the receiver. The Court stated that there is no guarantee that the message sent was the same message received. The Solicitor General pointed out that "the messages were transmitted to and received not by private respondent himself but his computer."[180] Second, the print-outs were not certified or authenticated by any company official who could properly attest that these came from the petitioner's computer system or that the data stored in the system were not and/or could not have been tampered with before the same were printed out. The Court took into account the fact that the computer unit and system were in the exclusive possession and control of the company after the respondent was served his termination letter.[181]

In subsequent cases,[182] the Court only made reference to emails as basis for the arguments of the parties. It did not go in depth in discussing how the authentication, or attribution was made by the parties.

---

[179] G.R. No. 117221, 305 SCRA 592, Apr. 13, 1999.

[180] *Id.*

[181] *Id.*

[182] Intel Technology Philippines v. NLRC, G.R. No. 200575, 715 SCRA 514, Feb. 5, 2014; Auza v. Mol Philippines, G.R. No. 175841, 686 SCRA 66, Nov. 21, 2012; *In Re* Writ of Amparo and the Writ of Habeas Data in Favor of Melissa Roxas v. Gloria Macapagal-Arroyo, G.R. No. 189155, 630 SCRA 211, 239, Sept. 7, 2010; Pollo v. David, G.R. No. 181881, 659 SCRA 189, Oct. 18, 2011; Unilever Philippines, Inc. v. Rivera, G.R. No. 201701, 697 SCRA 136, June 3, 2013; Hechanova Bugay Vilchez Lawyers v. Matorre, G.R. No. 198261, 707 SCRA 570, Oct. 16, 2013; Acesite Corp. v. NLRC, G.R. No. 152308, 449 SCRA 360, Jan. 26, 2005; Punzal v. ETSI Technologies, Inc., G.R. No. 170384-85, 518 SCRA 66, Mar. 9, 2007; United Philippine Lines, Inc. v. Sibug, G.R. No. 201072, 720 SCRA 546, Apr. 2, 2014; Montinola v. Philippine Airlines, G.R. No. 198656, 734 SCRA 439, Sept. 8, 2014; Torres v. Perez, G.R. No. 188225, 686 SCRA 615, Nov. 28, 2012; Reyes-Rayal v. Philippine Luen Thai Holdings Corp., G.R. No. 174893, 676 SCRA 183, July 11, 2012.

5. Chat room messages

The court has not had the occasion to discuss the authentication and admissibility of messages sent in chat rooms. This is unfortunate, particularly because most of the transactions on internet-facilitated sex trafficking, or entrapment operations are ironed out in chat sessions.

6. Facebook posts/messages

It was only in 2014, when a graduation scandal broke out in Saint Theresa's College, that Facebook posts and messages became part of a justiciable controversy. In *Vivares v. St. Theresa's College*,[183] two female minors who were graduating from high school took photos of themselves wearing only their brassieres. One of their friends uploaded the photos on Facebook. Several students who were Facebook friends with the minors saw the photos through their own accounts, they logged on to their Facebook accounts using the computers in the school computer lab and showed the photos to one of their teachers. The teacher brought the matter up before the school discipline committee, which decided that the girls were not allowed to march or attend the graduation ceremonies. The parents of the minors (petitioners), filed a petition for the issuance of a writ of habeas data, and prayed that the school be ordered to submit all printed and soft copies of the photos before the RTC.

Petitioners claimed that the teacher intruded into their children's accounts, downloaded copies of the pictures and showed it to the discipline committee. They also alleged that the photos were available to only five other friends of the girls and not to the public. Thus, the teacher's act was a breach of the minor's privacy since the privacy settings gave them a reasonable expectation of privacy. On the other hand, the respondent stated in her affidavit that it was the students in school who brought the photos to her attention while using the computer lab. She claimed that the students even told her that some photos were set on "public".

The Supreme Court ruled in favor of the teacher and Saint Theresa's College stating that it was the minor's friends who showed the pictures to the teacher. The school was the mere recipient of the information and it did not resort to any "unlawful means of gathering the information as it was voluntarily given to them by persons who had legitimate access to the posts.[184]" More importantly, the photos were set on "friends only", which cannot be said to be "very private" as claimed by the petitioners.

---

[183] *Vivares*, 737 SCRA 92.

[184] *Id.*

In this case, the respondent printed out a copy of the photos and submitted it to the court. Unfortunately, there was no discussion on the authentication of the posts or the photos themselves. It was unnecessary because the uploader was identified as one of the friends of the minors, and it was never put in issue by the parties.

In 2011, a libel case filed by Dr. Vicky Belo's Medical Group Inc. ("BMGI") against Atty. Argee Guevarra for alleged libelous statements posted on Facebook was dismissed by the RTC due to improper venue.[185]

1. Websites

In *Bonifacio v. RTC Makati*,[186] a criminal complaint for libel was filed against several accused. The accused were a large group of disgruntled pre-need plan holders in a corporation owned by petitioners. They were unable to collect on their plans since the corporation had liquidity concerns and underwent corporate rehabilitation. The accused operated a blog, and a Yahoo! e-group as a common platform for plan holders to seek redress. These websites were readily available to the public. Unfortunately, similar to the BMGI case, the petition was dismissed due to improper venue.

Publication through online websites is not the appropriate medium for publishing laws, rules and regulations, this was discussed in the case of *Garcillano v. House of Representatives.*[187] The respondents invoked the E-Commerce Act to support their claim of valid publication of the Senate Rules of Procedure Governing Inquiries in Aid of Legislation. The Supreme Court rejected their claim of valid publication. In ruling, the Court stated "R.A. No. 8792 considers an electronic data message or an electronic document as the functional equivalent of a written document only for *evidentiary purposes.* In other words, the law merely recognizes the admissibility in evidence of electronic data messages and/or electronic documents. It does not make the internet a medium for publishing laws, rules and regulations."[188]

In the labor case of *Colegio de San Juan de Letran-Calamba v. Tardeo*,[189] the respondent made a request for fund assistance from the College for a

---

[185] Karen Flores, *Court junks PH's first Facebook libel case*, July 26, 2011, ABS-CBNNEWS.COM, *at* http://news.abs-cbn.com/lifestyle/07/26/11/court-junks-phs-first-facebook-libel-case.

[186] G.R. No. 184800, 620 SCRA 268, May 5, 2010.

[187] G.R. No. 170338, 575 SCRA 170, 185, Dec. 23, 2008.

[188] *Id.*

[189] G.R. No. 190303, 729 SCRA 497, July 4, 2014.

seminar. In her letter request, she attached an invitation allegedly downloaded from the website of the organizers. The invitation detailed the expenses for the upcoming seminar. During pre-audit, the Vice-President for Finance noted that the supporting documents appeared to have been taken from the website, but it was altered and significant portions were missing which led him to conclude that the parts were deliberately omitted by the respondent. She was dismissed for dishonesty and misconduct. The Supreme Court ruled that she was unlawfully dismissed because there was no showing that the alteration of the documents from the website amounted to serious misconduct.

Lastly, in the case of *SPI Technologies, Inc. v. Mapua*,[190] the respondent filed a complaint for illegal dismissal against the petitioner. The petitioner claimed that it had to let her go on the ground of redundancy. She negated the claim and presented two advertisements in classified websites for job vacancies for positions with the exact same job description as her former job. The advertisements themselves were not presented, instead the respondent executed an affidavit based on the website advertisement. The court did not definitely rule on the admissibility of the website posting based on the affidavits, however the issue became moot and academic because the corporation admitted to posting the job advertisements.

To synthesize all the information in the cases discussed, the author compiled a list of the manners in which the evidence was authenticated by the counsels in their respective cases.[191]

C. Rules on electronic evidence as applied in the United States

Philippine case law on electronic evidence is still at its infancy, particularly as regards prosecuting internet-facilitated sex trafficking. There is only one decided case on Facebook postings, no cases on chat room logs, and the single case with an extensive discussion on email authentication was decided even before the REE.

Consequently, the author looked to the Federal Rules of Evidence (FRE) of the United States, which is the basis of our REE. Moreover, the Philippine Supreme Court Committee on Revision of Rules even requested the American Bar Association Asia Law Initiative ("ABA-Asia") to assess the sufficiency of the REE and to make recommendations if necessary, thus an examination of U.S. jurisprudence applying the rules would be proper.

---

[190] G.R. No. 191154, 720 SCRA 743, Apr. 7, 2014.

[191] *See* Appendix D, "Selected forms of electronic evidence as classified and properly authenticated under the Rules on Electronic Evidence."

1. Electronic mail/ email

U.S. courts have declared that if the email contains sufficient personal details,[192] the typewritten name or nickname of the recipient or the sender, or the use of an email address which many times contains the name of the sender, this is adequate proof of authentication. In *State v. Pullens*,[193] the accused was suspected of murdering his mother. After he was taken into custody and later released, he exchanged numerous emails with a police officer investigating the case. The officer presented the emails in court and the evidence was admitted over the objections of the accused. The messages came from various email addresses: stephenpullens@yahoo.com signed "Stephen Pullens," pullens_ stephen@yahoo.com signed "Stephen Pullens" or "Stephen Pullens or friends thereof." Another email was from grid_works@ureach but was signed "Stephen Pullens" and "this is not Stephen." A computer forensics expert testified that he was able to determine what email addresses were used from the computer in the mother's apartment at the time the accused was staying there immediately before her death. Another detective testified that he was assigned to compile and verify all the information from the emails received. The information gathered from the emails included the layout of the mother's apartment, the accused's previous travel, prior residence, prior employment, schooling, sports activities and girlfriends.

The acts of the defendant himself may serve to authenticate emails, together with an affidavit of the custodian of records of an internet service provider, stating that the login name was registered to the defendant. In *Commonwealth v. Amaral*[194] the defendant was convicted of attempted rape of a child and solicitation of a prostitute posing as a fifteen-year-old through Craigslist, an online bulletin board. The prosecution presented email communications between the accused and an undercover officer posing as a minor prostitute, printed in chronological order. The defendant argued that they were not properly authenticated and did not conform to the best evidence rule. The court admitted email printouts from rdwmercury2006@yahoo.com in evidence after the prosecution presented two pieces of evidence.

First, the acts of the defendant served to authenticate the emails. The accused indicated that he would be at a certain place at a certain time, and he appeared at that place and time. He also gave his telephone number and

---

[192] *See* United States v. Siddiqui, 235 F.3d 1318, 1322-23 (11th Cir. 2000); See also United States v. Safavian, 435 F. Supp. 2d 36, 40 (D.D.C. 2006); Shea v. State, 167 S.W.3d 98, 105 (Tex. App. 2005).

[193] State v. Pullens, 281 Neb. 828, 860, 800 N.W.2d 202, 229 (2011).

[194] 78 Mass. App. Ct. 671, 674-75, 941 N.E.2d 1143, 1147 (2011).

photograph through the email, when the state trooper called the number, the defendant immediately answered his phone, and when they met up in the entrapment operation the photograph the accused had sent was an accurate picture. Second, the prosecution presented an affidavit from the custodian of records of Yahoo! Inc., the affidavit indicated that the login name of rdwmercury2006@yahoo.com was registered to the defendant. The affidavit was accepted as a business record, an exception to the hearsay rule. The court explicitly stated that this affidavit alone was relatively weak in weight, however when considered in conjunction with the other evidence presented, there was sufficient authentication for admission.

The electronic signature of an employee was considered in admitting an email under the U.S. hearsay exception of admission of a party opponent, or an admission against interest.[195] In *Sea-Land Service, Inc. v. Lozen Intern., LLC*[196] the district court excluded an internal company email authored by employee A and sent to employee B. Employee B forwarded the email to the defendant, and defendant attempted to admit it into evidence. The court excluded the email since defendant did not present evidence to indicate the identity or job title of employee A, who allegedly authored the email. The court reversed the decision and admitted the email since it contained an electronic "signature" attesting that the email was authored by employee A and concerned a matter within the scope of his employment. The email was considered 'an admission by a party opponent,' this is the U.S. equivalent of the Philippine rule on admission against interest, or a statement made by a party's agent or servant concerning a matter within the scope of the agency or employment, made during the existence of the relationship.

2. Text messages (SMS)/ Multimedia (MMS)

In the case of *Dickens v. State*[197] the accused fatally shot his wife and the only issue was whether it was premeditated murder or a lesser degree of culpable homicide. The prosecution presented in evidence five threatening text messages allegedly sent by the accused to his deceased wife before she was killed. The mother of the victim testified that a few days after the murder, she took possession of her daughter's cellphone and scrolled through the text messages. She read the messages sent by the accused then contacted the detective assigned to the case who took photographs of each of the messages. The photographs were introduced into evidence as State exhibits. The Mary-

---

[195] *See* Dominion Nutrition, Inc. v. Cesca, 2006 U.S. Dist. LEXIS 15515, at *16 (N.D. Ill. 2006); Sklar v. Clough, 2007 U.S. Dist. LEXIS 49248 (N.D. Ga. 2007).

[196] 285 F.3d 808 (9th Cir. 2002).

[197] 175 Md. App. 231, 237-41, 927 A.2d 32 (2007).

land court admitted the messages, since they contained details that only few people would know about such as a reference to a particular movie the couple liked and their wedding vows. Furthermore, it was proven that the defendant had the phone in his possession when the messages were sent therefrom.

Expert testimony was presented in the case of *State v. Taylor*[198] where the victim, driving a 1998 Ford Contour, was murdered after setting up a scheduled rendezvous with the defendant through text messaging. A strategic care specialist from the phone company, Nextel, and the manager of the company that owned and issued the cellphone that the victim was using at the time of the murder, testified at trial. The text messages were admitted because both witnesses had knowledge of how Nextel sent and received text messages and how these were stored and retrieved. This testimony was sufficient to authenticate the State's exhibits of text messages sent to and from the victim's assigned Nextel cellphone number on the date of the murder. The defendant argued that no showing was made of who actually typed and sent the text messages. The court dismissed his objection on the ground that the text messages contained sufficient circumstantial evidence that tends to show that the victim was the person who sent and received them. The messages included information that the person would be driving a 1998 Contour, and the sender self-identified himself twice as "Sean," the accused's first name.

Finally, in *People v. Brown*,[199] a witness was presented to testify on text messages received through her cellphone from the accused. The prosecution introduced the messages into evidence by introducing the cellular phone itself as an exhibit, having the witness identify the phone, and read the messages from the telephone aloud. The witness testified that the messages came from the defendant, and were "signed" in the defendant's name.

3. Internet Websites

In authenticating websites, the courts have not applied a uniform standard. The requirements have generally fallen into three categories: (1) information from the website master or someone with personal knowledge that the information was posted by the individual; (2) an affidavit from the person who took the screenshot stating that the photo accurately reflects the data on the website; and (3) the last category requires proof that the post was actually uploaded on the site by its author.[200]

---

[198] 178 N.C. App. 395, 412-15, 632 S.E.2d 218 (2006).

[199] A122791, 2009 WL 1878704, at *3 (Cal. Ct. App. 2009).

[200] Allison L. Pannozzo, *Uploading Guilt: Adding a Virtual Records Exception to the Federal Rules on Evidence*, 44 CONN. L. REV. 1709 (2012).

A high standard was set in the case of *Wady v. Provident Life and Accident Insurance Co.*[201] The plaintiff filed a claim against the insurance company for breach of contract after it disallowed her disability insurance claim. Plaintiff presented six exhibits which she claimed to have obtained from the defendant's website on April 9, 2002. The defendant objected on the grounds that the plaintiff has no personal knowledge of who maintains the website, who authored the documents, or the accuracy of their contents.[202] The court ruled in favor of the defendant.

In *St. Clair v. Johnny's Oyster & Shrimp, Inc.*,[203] the court minced no words when it said "the Court holds no illusions that hackers can adulterate the content on any web-site, from any location, at any time. For these reasons, any evidence procured off the internet is adequate for almost nothing."[204] The court instructed the plaintiff to look for admissible documentation to support her claim instead of referring to the "voodoo information taken from the Internet". Note, however, that the *St. Clair* decision was made in 1999. The court may have taken a more progressive stance since then.

In the case of *Nightlight Sys., Inc. v. Nitelites Franchise Sys., Inc.*[205] a lower standard was established. The court ruled that there was no need for authentication from the website administrators themselves. It was sufficient that the proponent testify that the screenshot of the generic website accurately reflects what was on the site when he logged on to it. In this case, the plaintiffs filed a complaint against the defendant for infringement of its patent for creating custom electronic audio greeting cards via computer. They presented screenshots of a website that redirected users to another website. The defendant objected to the admission of the evidence for lack of foundation. The declaration of the witness was that he personally logged on to the website and is competent to testify as the user of the site. The court admitted the screenshots, stating that "although the witness does not have knowledge as to how the website works on a technological level, his declarations establish sufficient knowledge to attest that the screenshots are an accurate representation of what he encountered upon visiting the website."[206] The same approach was taken by the court in *United States v. Standring*.[207]

---

[201] Am., 216 F. Supp. 2d 1060, 1064-65 (C.D. Cal. 2002).

[202] *See also* Moroccanoil v. Marc Anthony Cosmetics, F.Supp.3d (2014).

[203] 76 F.Supp.2d 773 (1999).

[204] *Id.*

[205] 2008 WL 4906115, at 1 (C.D. Cal. 2008).

[206] *Id.; See also* Victaulic Company v. Tieman, 499 F. 3d 227 (2007).

[207] 2005 U.S. Dist. LEXIS 41330 (S.D. Ohio 2006).

Lastly, in the fascinating case of *United States v. Jackson*,[208] the accused attempted to rip off the United Parcel Service in a scheme that included sending hate mail to African-Americans. The accused wanted to introduce into evidence web site postings in which the white supremacist groups "gloat about the Jackson case, take credit for the racist United Parcel Service (UPS) mailings, and discuss the McCall bomb scare." The court excluded the screenshots presented in evidence because the accused failed to prove that the website postings were actually posted by the white supremacist groups to which she attributed it. She then attempted to fit the screenshots under the hearsay exception, as business records of the Internet Service Providers (ISPs). The court noted that she presented no evidence that the ISPs posted the messages websites or monitored the contents of those sites. The fact that the ISPs may be able to retrieve information or emails that its customers posted or sent does not turn that material into a business record of the ISP.

4. Internet archives

One of the unique features of websites is that their contents do not remain static, the web master can easily update photos or messages. Generally, these changes are not recorded on the website. This poses a challenge to litigators who have to prove the contents of the website at the time the cause of action arose.

For instance, in the example given earlier in Part III on acquiring jurisdiction over offenders, the prosecutor can show the court what appears on the website http://www.otonanojikan.com when a customer logs on from Japan[209] as part of the evidence to establish the maintenance of a cybersex den. When the web administrators become aware of the investigation, they can delete the website or change the contents without notice. At first blush, this may seem detrimental to the prosecutor's case, however modern technology has developed a solution to this. To solve this, lawyers can obtain internet archive services. These services provide snapshots of the web page at various points in time, including the critical time in question.

In *Telewizja Polska USA, Inc. v. Echostar Satellite Corp.*,[210] the plaintiff sued the defendant for trademark infringement. The defendant continued to use the license to market its subscription package to customers even after the expiration of the agreement. In its defense, the defendant sought to include screenshot printouts from the plaintiff's website from the Internet Archive's

---

[208] 208 F.3d 633 (7th Cir. 2000).

[209] Cabanlong, *supra* note 65.

[210] 2004 WL 2367740, 65 Fed. R. Evid. Serv. 673 (N.D. Ill. 2004).

"Wayback Machine." The Wayback Machine[211] allows a user to obtain an archived web page as it appeared at a particular moment in time. The screenshots were admitted after the defendant submitted an affidavit from an Internet Archive employee, who verified "that the Internet Archive Company retrieved copies of the website as it appeared on the dates in question from its electronic archives."[212] This affidavit requirement was reiterated in the case of *St. Luke's Cataract and Laser Institute, P.A. v. Sanderson*[213] where the exhibits introduced by the plaintiff were excluded for lack of authentication. In so holding, the court declared, *viz.*:

> to show that the printouts from Internet Archive are accurate representations of the ... websites [at issue] on various dates since 2000, Plaintiff must provide the Court with a statement or affidavit from an Internet Archive representative with personal knowledge of the contents of the Internet Archive website.... [A]n affidavit by ... [a] representative of Internet Archive with personal knowledge of its contents, verifying that the printouts Plaintiff seeks to admit are true and accurate copies of Internet Archive's records would satisfy Plaintiff's obligation to this Court.[214]

5. Messages in chat rooms and social networking sites

In the case of *State of Connecticut v. Eleck*,[215] the defendant claimed that the lower court erred in excluding from evidence a Facebook printout documenting electronic messages sent to him by a victim from her Facebook account after the assault. The defense counsel showed the victim a printout of the alleged exchange of electronic messages between the defendant's Facebook account and another account under the user name "Simone Danielle". The victim identified the user name as her own, but denied sending the messages. She claimed that someone hacked into her account and changed her password, thus she had no to access it at the time the messages were allegedly sent. The state objected to the admission of the Facebook print outs

---

[211] The Wayback machine is an internet-based service provided by Internet Archive, a 501(c)(3) non-profit organization. Internet Archive was founded in 1996 with the purpose of building an Internet library that offered permanent access for researchers, historians, and scholars to historical collections that may exist only in digital formats; *See* Discovery Practices and Procedures Subcommittee of the Enforcement Committee, *Wayback Machine Memo*, Nov. 2, 2009, http://www.inta.org/Advocacy/Documents/INTAWaybackMachine2009.pdf.

[212] *Id.*

[213] No. 8:06-cv-223-T-MMS, 2006 WL 1320242 (M.D. Fla. 2006).

[214] *Id.*

[215] 23 A.3d 818 (Conn.App. 2011).

on the ground that the authorship of the messages could not be authenticated. To attempt to authenticate the document, the defendant testified that he downloaded and printed the exchange of messages directly from his computer, that he recognized her user name as belonging to the victim because she added him as a Facebook friend, and that the Facebook profile contained photographs and other entries identifying her has the holder of the account. The court declined to admit in evidence the printouts on the ground that the defendant had failed to authenticate that the messages were written by the victim herself.

This doctrine was similar to the finding in the case of *Commonwealth v. Purdy* [216] where the court stated that evidence that the electronic communication originates from social networking website or from email that bears the alleged author's name is not in itself sufficient to authenticate the message. The user names are only treated as circumstantial evidence of authenticity and can only be admitted if supported by other circumstantial evidence. Apart from the actual message or letter itself, there must be proof that the reply probably came from the addressee of the letter.[217]

In several cases, the courts declared that an expert witness could be resorted to, to authenticate messages. The successful use of an expert witness was illustrated in the case of *People of New York v. Clevenstine*[218] wherein the defendant befriended a family and used that relationship to gain access to the family's two teenaged daughters. There was an exchange of sexually explicit messages between the defendant and the girls on Myspace. To authenticate the Myspace messages, an investigator from the computer crimes unit testified that he retrieved the conversations from the hard drive of the computer used by the victims, and an officer from Myspace explained that the messages on the computer disk had been exchanged by users of the accounts created by the defendant and the victims.

In *Commonwealth v. Williams*,[219] the court did not admit the Myspace messages that were printed out in the courthouse and testified to by the recipient. The judge stated that there was no expert testimony to the effect that no one other than the alleged sender that could communicate from that webpage.

Interestingly, the fact that a third party read the messages, and testified to having read them (in conjunction with other supporting evidence) was

---

[216] 459 Mass. 442, 450, 945 N.E.2d 372 (2011).

[217] Griffin v. State, 419 Md. 343, 363–64, 19 A.3d 415 (2011).

[218] 68 A.D.3d 1448, 891 N.Y.S.2d 511 (2009).

[219] 456 Mass. 857 (2010).

sufficient for authentication. In the same case of *People of New York v. Clevenstine*,[220] the wife of the defendant accidentally discovered the saved instant message communications in his Myspace account. She filed the complaint with the police and testified to having read the sexually explicit communications while on their home computer. The court declared "such testimony provided ample authentication for admission of this evidence."[221]

In *United States v. Tank*,[222] the court admitted the chat room conversation in evidence when the defendant admitted that he participated in said conversation using the screen name "Cessna." Several co-conspirators also testified that he used that name, and defendant showed up at a subsequent meeting in person, arranged by a person using the screen name "Cessna".

In *United States v. Simpson*,[223] a chat room print out was admitted in evidence when an individual using the handle name "Stavron" gave the officer the defendant's name and address and subsequent email exchanges indicated that the email address belonged to defendant.

6. Posts on Social Networking sites

In the recent 2014 case of *United States v. Hassan*,[224] the court admitted screenshots of Facebook postings authenticated through the business records exception. It must be noted, however, that the court only acted as a gatekeeper. The merits of the case were decided on by a jury. Two men were tried and convicted of several offenses arising from terrorism activities.

The prosecution presented exhibits consisting of screenshots of the Facebook pages and postings of the accused men, taken at different points in time. The prosecution supplemented these screenshots with information they had taken from the Facebook pages, such as their personal biographical information, quotations, listings, interests, and the postings of others on their "walls". The pages were also linked to the mailing and email addresses of the accused via their internet protocol (IP) addresses. The government presented certifications of the records custodian of Facebook. The custodian verified that the Facebook pages had been maintained as business records in the course of regularly conducted business activities. The records were created and retained soon after the users posted them through the Facebook servers.

---

[220] 68 A.D.3d 1448, 891 N.Y.S.2d 511 (2009).

[221] *Id.*

[222] 200 F.3d 627, 630-31 (9th Cir. 2000).

[223] 152 F.3d 1241, 1249-50 (10th Cir. 1998).

[224] 742 F.3d 104 (4th Cir. 2014).

This is in sharp contrast to the case of *Moroccanoil v. Marc Anthony Cosmetics*[225] where the defendant was sued for trademark infringement. In its defense, the defendant attempted to present mere Facebook screenshots. The court denied the screenshots and ruled that they were inadmissible without supporting circumstantial information. This same doctrine was reiterated in the case of *Commonwealth v. Banas.*[226]

The case of *United States v. Vayner*[227] is helpful to illustrate the danger of this careless practice of relying on mere screenshots that result in wrongful convictions. In that case, the judgment of conviction for unlawful transfer of a false birth certificate was vacated on appeal. The lower court admitted a mere screenshot of the defendant's alleged www.VK.com profile (the Russian version of Facebook) and used this as basis to convict the accused. The alleged profile page established the key connection between the defendant and another perpetrator who became state witness.

Another method by which Facebook, Myspace or online profile content may be authenticated is through the distinct characteristics, substance, photos, and the timing activities of the user. In *United States v. Grant*[228] the defendant was convicted in part due to his Facebook messages. All the messages contained his name and were accompanied by a picture of the accused. The content in the messages also served to provide additional information, such as his phone number and flight information. The accused also added the victim on Facebook, and sent her the messages in question immediately after they met.

In determining the authenticity of the Facebook messages, the court in *Campbell v. Texas*[229] took into account the unique speech pattern of the defendant, the private nature of the communications and his electronic signature included in the messages.

In *Griffin v. Maryland*,[230] the accused made a threatening statement on his girlfriend's Myspace page. The posts on her page were printed and submitted to the court for admission into evidence. When his girlfriend took the stand, she was not questioned on the authenticity of the posts, later his counsel objected to the admission of the posts. The court allowed the

---

[225] F.Supp.3d, (2014).

[226] 2014 WL 1096140 (2014).

[227] 2014 WL 4942227 (C.A. 2 (N.Y.) 2014).

[228] No. ACM S31758, 2011 WL 6015856 (A.F. Ct. Crim. App. 2011).

[229] No. 03–11–00834–CR (Tex. Ct. App. 2012).

[230] 192 Md. App. 518, 995 A.2d 791 (2010).

inclusion of the Myspace posts into evidence on the following grounds: There was a picture on her profile linking it to the defendant, an accurate birth date, reference to the defendant's nickname, and a reference to the correct number of children.

7. Videos uploaded to YouTube and other websites.

In the same case of *Hassan*[231] the government also presented a video posted by one of the accused on www.RossTraining.com depicting him doing physical training exercises in a video that opened with a series of quotations onscreen such as "[t]here is no God but ALLAH and Muhammad is his Messenger." The video was retrieved from Google's server. Similar to the Facebook postings, the government presented a certification from that records custodian of Google verifying that the video had been maintained as business records, shortly after it was posted by one of the accused. The court admitted the video into evidence.

Similar to what was done for Philippine jurisprudence, the author synthesized all the information in the cases discussed and how authentication was carried out for the different modes of electronic evidence. Specific cases were chosen to illustrate methods by which authentication can be performed, the list below is by no means an exhaustive list of U.S. jurisprudence on electronic evidence.

D. Synthesis, analysis, and recommendations

There is much confusion as to the proper presentation and authentication of electronic evidence. Since the DOJ and the Office of Cybercrime have yet to develop a comprehensive module on electronic evidence, the author drafted a basic framework that could be used to guide prosecutors on the fundamental rules of authentication of electronic evidence. This framework is by no means exhaustive, and is intended as a starting point for further development.

The framework consists of two parts. The first part lists the modes of electronic evidence used in internet-facilitated sex trafficking, and their proper classification and mode of authentication under the REE. The second part is a comprehensive summary of Philippine and U.S. jurisprudence on the topic, with analysis on how the rules can be applied in the country to prosecute internet-facilitated sex trafficking.

---

[231] 742 F.3d 104 (4th Cir. 2014).

1. Forms of electronic evidence and their classification under the REE[232]

An attorney seeking to prosecute a case on internet-facilitated sex trafficking must first hurdle the problem of authentication. If the lawyer is presenting object evidence (e.g.: a photograph of the cybersex den), he/she must provide foundational evidence to show that the object is the real thing, and not a mere substitute or representation of the real thing.[233] The same is also true for documentary evidence (e.g.: an exchange of emails with details for payment), where the document is offered as proof of its contents.[234] The REE explicitly provides that an electronic document is the functional equivalent of a paper-based document.[235] It is therefore understood that when the proponent introduces electronic documentary evidence, the best evidence rule,[236] the parole evidence rule,[237] and the hearsay rule come into play. These rules find no application in object evidence.

Note that for both types of evidence, the REE provides a catch-all phrase for authentication. Ephemeral electronic communication can be proven by "other competent evidence"[238] and electronic documents can be introduced by "other evidence showing its integrity and reliability."[239] Research on methods of authentication in other jurisdictions can be useful, provided that it meets the standards of competency, integrity and reliability.

2. Comprehensive Summary of Philippine and U.S. jurisprudence on Electronic Evidence

The following summary is an exhaustive and complete depiction of all Philippine cases based on the 42 decided cases from 1999 to 2014, whereas the U.S. summary provides a selection of cases that are most applicable to prosecuting online crimes of a sexual nature. Prosecutors can use this as a reference in determining how to present a particular piece of evidence:

---

[232] *Supra* note 191.

[233] Willard Riano, Evidence: The Bar Lectures Series 147 (2009).

[234] *Id.*, at 183.

[235] REE, Rule 2, § 1(h).

[236] RULES OF COURT, Rule 130, § 3.

[237] § 9.

[238] Rule 11, § 1.

[239] Rule 5, § 2.

1. **Text messages (SMS) and multimedia messages (MMS)**
   a. The recipient of the text message testifies on its contents.
   b. A third party reads the messages on the cellphone of the recipient in the presence of the accused and of his counsel.
   c. The sender admits to having sent the messages.
   d. The sender admits to being the owner of the cellphone number, that sent the messages.
   e. The acts of the sender serve to authenticate the messages.

2. **Email**
   a. The email print-outs are signed by the sender or the receiver.
   b. A certification is issued as to the authenticity or integrity of the data, or the computer system from which the email print-out is made.

3. **Social networking sites**
   a. A person admits to having uploaded the photos.
   b. A third person testifies to having seen and read the posts through the accounts of other persons. Note however, that in this case the authenticity of the photos or the upload was not questioned.

4. **Chat rooms**
   No decided cases.

5. **Websites**
   The company admitted to uploading the posts and the contents of the website.

The REE are based, in part, on the FRE. It was for these reasons that the author turned to U.S. jurisprudence to assess how authentication was performed. In the United States, authentication of evidence is a two-step process. First, the judge makes a preliminary determination of authentication applying a low standard. It need only be shown that there is a rational basis for the jury to find that the evidence is authentic.[240] After this, the evidence is introduced during the trial and subject to cross-examination. It is the jury who assesses the evidence and makes the final determination of the authenticity and probative value.[241] Thus, in the cases below, if evidence was admitted by the judge based on Rule 901(a) of the FRE, it should be remembered that the court applied the lowest standard. A summary of the results is provided below:

---

[240] Federal Rules of Evidence, Rule 901(a).

[241] Griffith, *Understanding and Authenticating Evidence from Social Networking Sites*, 7 WASH. J.L. TECH. & ARTS 209 (2012).

1. **Email**
   a. The email contains sufficient personal details that identify the sender.
   b. The email address contains the name of the sender, and is signed with his electronic signature.
   c. An expert witness testifies that the email was sent from a computer that the sender had access to at the time of mailing.
   d. The acts of the sender served to authenticate the emails.
   e. Personal details or photos given by the sender through email are proven to be true, and match the sender after a meet-up in person.
   f. The custodian of records of the email company executes an affidavit that the log-in name in the email address is registered to the sender (business records exception to the hearsay rule).
   g. An email was forwarded by a party opponent (an admission against interest - exception to the hearsay rule).

2. **Text messages (SMS) and multimedia messages (MMS)**
   a. A third person testifies to having read the message in the phone of the recipient.
   b. Photographs are taken of the text messages in the cellphone of the recipient and presented in court with corroborating messages.
   c. The text message contains sufficient personal details that identify the sender, and includes details that are only known to the sender and the recipient.
   d. Proof is presented to show that the cellphone was in the exclusive possession of the sender at the time the messages were sent, and corroborated by other information
   e. An expert witness from the cellular service provider testifies as to how the service provider sent, received, stored and retrieved text messages
   f. The sender includes his/her name in the messages, the messages were "signed."
   g. The recipient testifies in court as to the contents of the message.

3. **Websites**
   a. The website administrators are presented to authenticate the contents of the page. These administrators have knowledge of how the website works on a technological level.
   b. The author of the content is clearly identified and presented.
   c. Testimony is presented to prove that the screenshot was taken by a person who actually logged on to the website, and that the screenshot is an accurate depiction of what he/she saw. This is useful particularly for generic websites, but not for pages in social networking sites that are subject to frequent changes.

4. **Internet archives**
   a. An affidavit of the internet archive employee is presented to verify that the company retrieved the copies of the website on the specific dates in question, and that the copies presented are correct and accurate depictions of their files.
   b. A screenshot print-out of the website is presented; the screen-shot must depict the website as it appeared, on the exact date in question.

5. **Messages in chat rooms and other social networking sites**
   a. A print-out of the messages is presented together with proof that the sender actually authored the message; the mere fact that the message bears the alleged author's name is insufficient.
   b. Expert testimony is presented to give proof that no one other than the alleged sender could communicate from the webpage.
   c. An expert witness can certify that he retrieved the conversations from the hard drive of the computer used by the recipient or the sender.
   d. A third party who has read the message can testify to its contents if corroborated by other information sufficient to authenticate the same.
   e. The sender admits to using the screen name indicated in the messages, this admission may be corroborated by others who have personal knowledge of the chat room conversations.
   f. The sender gives personal details through the chat room, and the details are later proven to be true.

6. **Posts on social networking sites**
   a. A records custodian of the site verifies that the information on the webpages were maintained as business records in the course of regularly conducted business activities.
   b. Screenshots of the posts and profile are linked to the mail and email addresses of the person via his/her IP address.
   c. Mere screenshots are inadmissible; they must be presented with supporting circumstantial information.
   d. Information is presented with distinct characteristics (e.g., unique speech pattern), and the timing of the posts may be taken into account.
   e. The counsel can present personal information shared through the site that was later confirmed to be accurate.
   f. The electronic signature of the sender may be taken into account, together with other identifying information.

7. **Videos uploaded on YouTube and other sites**
   A records custodian of the search engine verifies that the fact of the video upload was maintained as a business record in the course of its regularly conducted business activities.

Prosecutors can turn to U.S. cases for methods of authentication, particularly when there is no precedent in our jurisdiction. Of course in every instance, the court will exercise its discretion to determine if the threshold requirements have been met for competence, and integrity of the evidence.

With respect to email, seeing as the only case[242] that definitively discussed authentication of emails was decided in 1999, or before the passage of the E-Commerce Act, decided U.S. cases on the matter can be a useful reference. As shown in *State v. Pullens*[243] lawyers can point to the distinctive personal characteristics or details sent through the email, or they can refer to the electronic signature and the name used for the account. The prosecutor can take a different route, and present an affidavit from the custodian of records of the email service provider stating that the log-in name in the email address is registered to the sender, as was done in *Commonwealth v. Amaral*.[244] This affidavit can be easily obtained since email service providers such as Google and Yahoo! maintain offices in the Philippines.

Vivares[245] was the first case to discuss Facebook posts. In that case, a person admitted to having uploaded the photos and the teacher testified to having seen and read the posts through the accounts of other persons. U.S. jurisprudence on Facebook posts and messages is well developed; courts have relied on distinctive characteristics of the sender,[246] and in other cases, screenshots of the site were taken and corroborated with information such as the Internet Protocol address.[247]

In *Campbell*,[248] the lawyers presented a records custodian from Facebook to testify that the information on the personal page was maintained as a business record. The author checked the Facebook site and found that the company can disclose account records, however an MLAT or letter rogatory may be required to compel the disclosure.[249] Facebook was incorporated in the United States, and the mailing address for requests is in California. There is an existing MLAT between the Philippines and the United States, the treaty states "assistance shall be provided without regard to

---

[242] *IBM*, 305 SCRA 592.

[243] 281 Neb. 828, 860, 800 N.W.2d 202, 229 (2011).

[244] 78 Mass. App. Ct. 671, 674-75, 941 N.E.2d 1143, 1147 (2011).

[245] *Vivares*, 737 SCRA 92.

[246] *Grant*, No. ACM S31758, 2011 WL 6015856 (A.F. Ct. Crim. App. 2011); *Campbell*, No. 03–11–00834–CR (Tex. Ct. App. 2012).

[247] 742 F.3d 104 (4th Cir. 2014).

[248] No. 03–11–00834–CR (Tex. Ct. App. 2012).

[249] Facebook Information for Law Enforcement Authorities, Facebook, *available at* https://www.facebook.com/safety/groups/law/guidelines, (last accessed June 6, 2015).

whether the conduct which is the subject of the investigation would constitute an offence under the laws of the Requested State."[250] Accordingly, the affidavit of the records custodian could be obtained to prosecute a violation of our laws on cybersex.

In the only decided Philippine case[251] on authentication of websites, the company itself admitted to posting the contents. This is unlikely to happen in a case on internet-facilitated sex trafficking. Authentication of these sites is crucial to show the chat websites that perpetrators log on to. Prosecutors can present a witness who took a screenshot of the website, the witness can testify that the photo is an accurate depiction of what he/she saw as done in *Jackson*[252] *and St. Clair*[253] If the web administrators find out that an investigation is ongoing, or that a case has been filed, they may delete the content. All is not lost as lawyers can still refer to internet archive services. These services provide snapshots of the web page at various points in time, including the critical time in question. It can be authenticated through the testimony of an internet archive employee as in *Wady*.[254]

Finally, with respect to messages sent through chat rooms, the court has not had the opportunity to discuss authentication. However, as shown in U.S. cases, law enforcers can testify that the logs were retrieved from the hard drive of the computers in the cybersex den, and a print-out of the messages may be presented with circumstantial evidence to prove that the sender authored the messages as done in *Eleck*.[255]

V. CONCLUSION, OTHER AREAS OF LAW, AND THE WAY FORWARD

In conclusion, with the recommendations to: 1) accede to the Budapest Convention; 2) enter into more MLATs; 3) extend the coverage of the listed crimes in existing MLATs; 4) make more aggressive use of current MLATS; 5) enter into more bilateral extradition treaties; 6) extend the coverage of the listed crimes in existing extradition treaties; 7) amend Sec. 26-A of R.A. No. 9208, as amended by R.A. No. 10364; and 8) present the classification and requisite rules and the comparative guide of Philippine and

---

[250] Extradition Treaty with the United States (1996), Art. 1(3).

[251] *SPI*, 720 SCRA 743.

[252] 208 F.3d 633 (7th Cir. 2000).

[253] 76 F.Supp.2d 773 (1999).

[254] Am., 216 F. Supp. 2d 1060, 1064-65 (C.D. Cal. 2002).

[255] Case No. AC 31581 (CT App. Ct. 2011).

U.S. jurisprudence on electronic evidence to prosecutors, the author respectfully submits that the Philippines will be able to successfully acquire jurisdiction over perpetrators located in other states, gain more information and evidence, and successfully present evidence to prosecute crimes on internet-facilitated sex trafficking.

Although the scope of the paper was limited to issues on jurisdiction and evidence, there are other areas that could be improved to address sex trafficking, particularly the role of the Department of Social Welfare and Development ("DSWD"), local government units ("LGUs"), and the need for rules on privacy and confidentiality in the proposed Cybercrime courts.

First, with respect to the DSWD and LGUs. Prosecuting parents or guardians who pimp their children through cybersex, has a devastating effect on the family. The parents are imprisoned and the children are often left to fend for themselves, eventually entering into illicit jobs or ending up in the streets. Current laws fail to address this issue and focus primarily on victims of child pornography. To illustrate, the Anti-Child Pornography Act of 2009 directs the DSWD to ensure that the victim is provided 'appropriate care, custody and support for recovery',[256] victims and their families are entitled to protection under the "The Witness Protection, Security and Benefit Act" and government agencies and LGUs are mandated to provide victims with emergency shelter, free legal aid, and educational assistance. There are no parallel programs for victims of cybersex. Moreover, none of the bills[257] crafted to address this issue make mention of services to heal, support and reintegrate these victims.

Second, with respect to the creation of special cybercrime courts manned by specially trained judges to handle cybercrime cases in R.A. No. 10175,[258] the implementing rules and regulations have not been released. Thus, there are no guidelines for the qualification and training of cybercrime court judges, and the jurisdiction of the court. However, one issue is clear - the need for protection of women and children.

R.A. No. 10175 punishes cybersex, child pornography, all crimes defined and penalized by the Revised Penal Code and special laws if committed by, through and with the use of information and communications technologies.[259] Accordingly, as long as the crime is committed with any of

---

[256] Rep. Act No. 9775 (2009), § 14.

[257] *Supra* note 47.

[258] Rep. Act No. 10175 (2012), § 21.

[259] § 6.

the devices enumerated in Sec. 6(d) of the Act, such as mobile phones, smart phones or other data processing devices, jurisdiction is immediately lodged in the cybercrime courts.

This disregards the exclusive original jurisdiction of Family Courts under the Family Courts Act of 1997. Family Courts are mandated to hear and decide criminal cases where one or more of the victims is a minor at the time of the commission of the offense,[260] violations of R.A. No. 7610 or the Special Protection of Children Against Child Abuse,[261] Exploitation and Discrimination Act, and cases of sexual abuse of women,[262] and abuse of children.[263]

Cybercrime courts will require a combined expertise of two distinct and separate fields: family law and cybercrime law. In each field, there is already a dearth of qualified and willing judges and prosecutors, the numbers will certainly fall further if both fields are combined.

Legislators and drafters of the IRR should take into account not only the aforementioned issues on jurisdiction and specialized training, but also the need to adopt the rules on privacy and confidentiality of proceedings[264] for cybercrime cases involving women and minors to ensure sufficient protection of the child and the family's dignity and worth.[265]

- o0o -

[260] Rep. Act No. 8369 (1997), § 5(a).
[261] § 5(j).
[262] § 6(k)(1).
[263] § 6(k)(2).
[264] § 12.
[265] § 12.

APPENDIX A: PNP Anti-Cybercrime Group – Cybercrime Offenses in the Philippines from 2010 to 2014[266]

CYBERCRIME OFFENSES	2010	2011	2012	2013	2014	TOTAL
A. Offenses against confidentiality, integrity and availability of computer data and systems						
Hacking of personal accounts	13	5	16	26	47	107
Website defacement/hacking	157	350	339	271	-	1,117
B. Computer-related offenses						
Identity theft	5	6	4	28	45	88
Internet fraud/scam	31	49	41	73	106	300
Credit card fraud	1	4	4	32	30	71
C. Content related offenses						
Libel	8	26	21	32	87	174
Harassment/threat	17	30	22	30	68	167
Pornography related	4	5	11	-	-	20
R.A. No. 9775 (Anti-Child Pornography Act)	-	-	-	9	9	18
D. Other crimes defined and penalized under special laws						
R.A. No. 7610 (Special Protection of Children Against Abuse and Exploitation Act)	1	1	2	1	9	14
R.A. No. 9208 (Anti-Trafficking in Persons Act)	0	1	0	5	2	8
R.A. No. 9262 (Anti-Violence Against Women and Children Act)	-	-	-	6	8	14
R.A. No. 9995 (Anti-Photo and Video Voyeurism Act)	-	-	-	36	60	96
E. Other offenses						
Others	6	4	0	10	46	66
TOTAL	243	481	460	559	517	2,260

[266] Procured on Jan. 13, 2015 from Angel Redoble, Member, National Advisory Council of the PNP Anti-Cybercrime Group.

APPENDIX B: Philippine MLATs with eight states, the ASEAN MLAT and selected provisions[267]

Country & Date of Entry into Force	Specific List of Crimes	General provision on type of crimes	Extradition/ Transfer of Custody
Australia (1993)	• Revenue (taxation & custom duties) • Foreign exchange control • Graft & corruption, unlawfully acquired property, bribery, frauds against public treasury, malversation • Forfeiture of confiscation of property in respect of an offense • Recovery of pecuniary liability in respect of an offense • Restraining of dealings in property, freezing of assets to satisfy a pecuniary liability imposed in respect of an offense	×	Desistance shall NOT include arrest or detention of any persons with a view to extradition, and execution in the requested states of judgments imposed in the requesting state
USA (1996)	×	• "criminal offenses and in proceedings related to criminal matters" • Assistance shall be provided without regard to whether the conduct which is the subject of the investigation would constitute an offence under the laws of the Requested State.	• Transfer of custody is permitted if the person consents and the central authority of both states agree • If the requesting state seeks the location or identity of persons, the requested state shall use its best effort to ascertain the locations or identity of the persons or items

[267] Note: The author was unable to find a copy of the MLAT with Taiwan, signed on April 19, 2013.

Hong Kong (2004)	• Internal matters related to revenue (taxation and customs duties) • Graft and corruption, unlawfully acquired property, bribery, frauds against public treasury, misappropriation or fraudulent conversion of public funds or property • Forfeiture or confiscation of property in respect of an offence • Dealing in property, freezing of assets, satisfy a pecuniary liability in respect of an offense • Other revenue matters but NOT in connection with non-criminal proceedings related thereto	×	Transfer of custody can be granted provided the person consents and the requesting party has guaranteed the maintenance in custody of the person and his subsequent return to the requested party
Korea (2008)	×	"any offense the punishment of which at the time of the request for assistance, falls within the jurisdiction of the competent authorities of the Requesting party"	• Assistance does NOT include extradition, arrest, or detention • Does not include the execution of criminal judgments • Does not include transfer of persons in custody • Does not include transfer of proceedings in criminal matters
Spain (2008)	×	"any offences the punishment of which falls within the jurisdiction of the judicial authorities of the requesting state"	Transfer in custody is granted if both the person and the Central Authority of the requested State consent to the transfer

		assistance shall be provided without regard to whether the conduct would constitute an offence under the laws of the Requested State. Except in the executing requests for searches & seizures and proceedings related to the forfeiture of assets, restitution and collection of finds	
Switzerland (2005)	×	"offences the punishment of which falls within the jurisdiction of the judicial authorities of the Requesting State"	"NOT apply in the case of extradition, arrest or location of persons accused or convicted of an offence; NOT apply to the execution of penal judgments"
China (2012)	×	"Mutual assistance in the investigation and prosecution of criminal offenses & in proceedings related to criminal matters"	"This treaty shall NOT apply to extradition of any person, and the execution of criminal judgments, verdicts or decisions rendered in the Requesting party"
United Kingdom (2012)	×	"widest possible measure of mutual assistance in the investigation, prosecution and suppression of criminal offenses & in proceedings related to criminal matters"	"person in the custody of the state shall be transferred… if he and the contracting states consent"
ASEAN (adopted in 2004; entry into force provided in Art. 31 of Treaty)	×	"widest possible measure of mutual legal assistance in criminal matters, namely investigation, prosecution and resulting proceedings"	ASEAN treaty does not apply to the arrest or detention of any person with a view to extradition of that person"

APPENDIX C: Philippine extradition treaties with ten states[268]

Country & Date of Entry in Force	Extraditable offense based on Penalty	Specific List of Offenses	General provision for extraditable offenses	Dual Criminality	Can refuse extradition of national
China (2006)	Punishable under the laws of both parties by imprisonment for a period of more than one year or a more severe penalty	×	×	✓	✓
Hong Kong (1997)	×	21 offenses of a sexual nature including rape, sexual assault, indecent assault, and unlawful sexual acts upon children; statutory offences; offences against laws relating to prostitution and premises kept for the purposes of prostitution	×	✓	✓
Korea (1993)	"Punishable under the laws of both contracting parties by deprivation of liberty for a maximum period of at least one year or by a more severe penalty"	×	×	General rule: Yes *Exception:* offence relating to taxation, customs duties, forex control	✓

[268] Note: The author was unable to find a copy of the extradition treaties with Micronesia (1994), Spain (2014) and India (2014).

USA (1996)	"Punishable under the laws of both Parties by deprivation of liberty for a period of more than one year, or by a more severe penalty"	×	×	✓	×
Australia (1991)	"Punishable under the laws of both contracting states for a period of at least one year, or by a more severe penalty"	×	×	✓	✓
Canada (1990)	"Punishable under the laws of both countries by imprisonment or other deprivation of liberty for a maximum period of at least one year or by a more severe penalty"	×	×	✓	✓
Thailand (1984)	"If extradition is requested for any crime encompassed by par. 1, 2, or 3 of this article and that crime is punishable under the laws of both Parties by imprisonment or deprivation of liberty for a period exceeding one year"	17 offenses rape, indecent assault; unlawful sexual acts with or upon minors under the age specified by the penal laws of both contracting parties	"extradition may be granted at the discretion of the Requested Party in respect of other crimes for which it can be granted according to the laws of both Contracting Parties"	✓	✓
Indonesia (1976)	"If extradition is requested for any crime encompassed by par. A, B, or C of this article by a deprivation of liberty exceeding one year, such crime shall be extraditable under the provisions of this treaty."	17 offenses rape, indecent assault; unlawful sexual acts with or upon minors under the age specified by the penal laws of both contracting parties	"extradition may be granted at the discretion of the Requested Party in respect of other crimes for which it can be granted according to the laws of both Contracting Parties"	✓	✓

Switzerland (1997)	"offenses punishable under the laws of both contracting states by imprisonment or deprivation of liberty for a maximum period of at least 1 year or by a more severe penalty. And to the extent permit-ted under the law of the requested state, where the person is to be extradited for an extraditable offense, extradition may also be granted in respect of offenses which are punishable under the laws of both contracting states by imprisonment or other deprivation of liberty for a period of one year or less or by a less severe penalty."	×	×	✓	✓
United Kingdom	"Offense is punishable under the laws of both states by a maximum sentence of at least 12 mos. imprisonment or other form of detention or by a greater punishment; or the person who extradition has been requested has been convicted by a court with a sentence of imprisonment or another form of detention of a term of 4 mos. or more has been imposed and the conduct is punishable under the laws of the Requested State by a maximum sentence of at least 12 mos. or greater"	×	×	✓	×

APPENDIX D: Selected forms of electronic evidence as classified and properly authenticated under the Rules on Electronic Evidence

Medium	Classification	Authentication
Electronic mail/ e-mail	Electronic document[269] or electronic data message[270]	Rule 5, Section 2 a. by evidence that it had been digitally signed by the person purported to have signed the same; or b. by evidence that other appropriate security procedures or devices were applied; or c. by other evidence showing its integrity and reliability
Text messages (SMS)/ Multimedia electronic messages (MMS)	Ephemeral electronic communication[271]	Rule 11, Section 1 Audio, video and similar evidence. a. shall be shown, presented or displayed to the court; and b. identified, explained or authenticated by 1. the person who made the recording; or 2. by some other person competent to testify on the accuracy thereof Ephemeral electronic communications a. shall be proven by 1. the testimony of a person who was a party to the same; or 2. has personal knowledge thereof b. In the absence or unavailability of such witnesses, other competent evidence may be admitted
Internet website	Electronic document or electronic data message	Rule 5, Section 2 a. by evidence that it had been digitally signed by the person purported to have signed the same; or b. by evidence that other appropriate security procedures or devices were applied; or

[269] REE, Rule 2, § (1)(h). "Electronic document" refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be proved and affirmed, which is received, recorded, transmitted, stored, processed, retrieved or produced electronically. 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. For purposes of these Rules, the term "electronic document" may be used interchangeably with "electronic data message."

[270] Rule 2, § (1)(g). "Electronic data message" refers to information generated, sent, received or stored by electronic, optical or similar means.

[271] Rule 2, § (1)(k). "Ephemeral electronic communication" refers to telephone conversations, text messages, chat room sessions, streaming audio, streaming video, and other electronic forms of communication the evidence of which is not recorded or retained.

		c. by other evidence showing its integrity and reliability
Live/unrecorded videos streamed through a website (e.g. Skype)	Ephemeral electronic communication	Rule 11, Section 1 Audio, video and similar evidence. a. shall be shown, presented or displayed to the court; and b. identified, explained or authenticated by 1. the person who made the recording; or 2. by some other person competent to testify on the accuracy thereof Ephemeral electronic communications a. shall be proven by 1. the testimony of a person who was a party to the same; or 2. has personal knowledge thereof b. In the absence or unavailability of such witnesses, other competent evidence may be admitted
Messages in chat rooms/through social networking sites	Ephemeral electronic communication	Rule 11, Section 1 Audio, video and similar evidence. a. it shall be shown, presented or displayed to the court; and b. identified, explained or authenticated by 1. the person who made the recording; or 2. by some other person competent to testify on the accuracy thereof Ephemeral electronic communications a. shall be proven by 1. the testimony of a person who was a party to the same; or 2. has personal knowledge thereof b. In the absence or unavailability of such witnesses, other competent evidence may be admitted
Facebook posts	Ephemeral electronic communication	Rule 11, Section 1 Audio, video and similar evidence. a. it shall be shown, presented or displayed to the court; and b. identified, explained or authenticated by 1. the person who made the recording; or 2. by some other person competent to testify on the accuracy thereof Ephemeral electronic communications a. shall be proven by 1. the testimony of a person who was a party to the same; or 2. has personal knowledge thereof b. In the absence or unavailability of such witnesses, other competent evidence may be admitted