

 with  and  present


AK PARA SA BETA

THE INTERNATIONAL CONFERENCE IN CEBU


Theme:

CYBERPROTECTION OF CHILDREN

Cyber Safety of Children:
Internet and Mobile Protection for Minors




AkoParaSaBeta
APSB2013



Simultaneous Symposium 1: Online Child Abuse (Part I): Definitions, Laws and Reporting, Initial Investigation

Manila Room, 2nd level Marco Polo Plaza
1:30 – 5:00 PM



AkoParaSaBeta
APSB2013




SAPP Lolita Lomanta

Moderator

- Senior Assistant Provincial Prosecutor, Cebu Province
- Family Court Prosecutor handling cases on Women and Children
- Faculty Member, Southwestern University- College of Law
- Commissioner, Provincial Women's Commission (PWC)-Cebu Province
- Member, Technical Working Group- PWC




AkoParaSaBeta
APSB2013



OBJECTIVES:

At the end of the symposium, the participants will be able to:

- 1) Define online child abuse and its different forms;
- 2) Cite pertinent laws that protect children from online child abuse and exploitation



AkoParaSaBeta
APSB2013

PROGRAM

TIME	TOPIC	SPEAKER
1:30 – 1:40 PM (10 mins)	Overview of symposium, objectives, introduction of speakers and reactors	Moderator
1:40 – 2:10 PM (30 mins)	Case X – Lessons from a Collaborative Rescue	Atty. Lawrence Aritao
2:10 – 2:50 PM (40 mins)	Definition of online child abuse; Overview of existing laws and policies that safeguard children against this type of exploitation.	ACP Robinson Landicho
2:50 – 3:30 PM (40 mins)	Agencies that should be involved and the need for strong collaboration among agencies	Dir. Monica Pagunsan
3:30 – 3:45 PM (15 mins)	Overview of the major impact of Online Sexual Exploitation of Children (OSEC) and need for Aftercare	Dr. Clara Nemia Antipala
3:45 – 4:00 PM (15 mins)	Aftercare Teaser	Dr. José Andrés Sotto
4:00 – 4:10 PM (10 mins)	Brief Reaction	Judge Nathaniel Andal
4:10 – 4:40 PM (30 mins)	Open Forum	Moderator
4:40 – 5:00 PM (20 mins)	Summary	Moderator

A K
PARA SA
BETA

REACTOR:

- **Judge Nathaniel Andal**

#AkParaSaBETA
APR2013



A K
PARA SA
BETA

Atty. Lawrence Aritao

Case X – Lessons from a Collaborative Rescue

- Director of Prosecution Development, International Justice Mission (IJM) Philippines (2015)
- Director of Legal Interventions, IJM Pampanga (2015)
- Director of Legal Interventions, IJM Cebu (2013-2014)
- Special Counsel for Interventions, IJM Manila (2008-2013)
- Legal Clerk, IJM Manila (2008)
- U.P. College of Law Class of 2007
- Ateneo De Manila University Class of 2002
- Proud Husband, Father, and Avid Coffee Drinker
- Enthusiast Photographer



A K
PARA SA
BETA

ACP Robinson Landicho

Definition of online child abuse; Overview of existing laws and policies that safeguard children against this type of exploitation

- Assistant City Prosecutor, Department of Justice, Office of the Prosecutor of Pasig City (2009-present)
- Technical Working Group Member, IRR RA 10175; Cybercrime Investigation Manual, Task Force on Cybercrime
- Member, Criminal Code Committee (2013-present)
- Member, Committee on the Revision of the 2000 Bail Bond Guide (2012-present)
- Professor, Philippine Christian University, College of Law (2011-present)
- Awardee, Certificate of Recognition by the Office of the City Prosecutor of Pasig City for his selfless and invaluable service by assisting his colleagues in resolving their pending cases which helped the office achieve an excellent rating for the Year 2013 (Awarded in 2014)
- Awardee, Top 5 Performers on disposition of all cases (RPI, SUM, INQ) with an average of 99.12%. Awarded by the Office of the City Prosecutor of Pasig City (2012)
- Member, Philippine Bar - Roll of Attorneys No. 49039



AK

PARA SA

BETA

Dir. Ma. Monica Pagunsan

Agencies that should be involved and the need for strong collaboration among agencies

- Director IV, Planning and Management Service, Department of Justice (DOJ) (2006-present)
- Member, Sub-Committees on Governance and Rule of Law and Peace and Security
- Sits in the Committee for the Special Protection of Children (CSPC), an interagency committee rendering technical assistance to the Chairperson-designate
- Member, Technical Management Group, Council for the Welfare of Children (CWC)
- Member, DOJ Technical Working Group, United Nations on Convention Against Corruption (UNCAC) Compliance Committee
- Alternate member representative of the DOJ to the Interagency Council on Violence Against Women and their Children (IACVAWC), the council tasked to oversee the implementation of Violence Against Women and their Children Act



AK

PARA SA

BETA

Dr. Clara Nemia Antipala

Overview of the major impact of Online Sexual Exploitation of Children (OSEC) and need for Aftercare

- Director of Aftercare, International Justice Mission – Cebu
- Former Assistant Regional Director for Operations, DSWD 7
- Holds the following academic degrees: Doctor in Public Administration, Cebu Normal University (2008); Master of Science in Social Work, University of Southern Philippines, Cebu (1995); Bachelor of Arts in Psychology, University of San Carlos, Cebu City, Philippines (1974)



AK


PARA SA

BETA

Dr. José Andrés Sotto

Aftercare Teaser

- Consultant for Aftercare Development, IJM
- Practicing Trauma Therapist and Pastoral Counselor
- Special Areas of Study: Male Victims/Survivors of Sexual Abuse and Burnout Among Human Service Workers
- Certified Suicidologist, USA and Canada
- Trainer, Trauma-Informed Care and Trauma-Informed Psychotherapy



AK


PARA SA

BETA

Brief Reaction

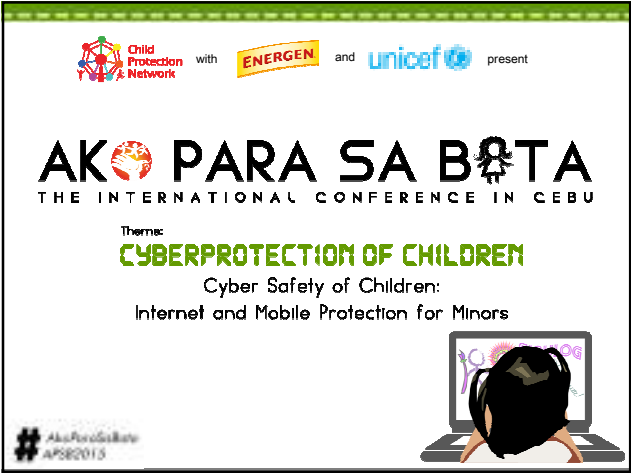
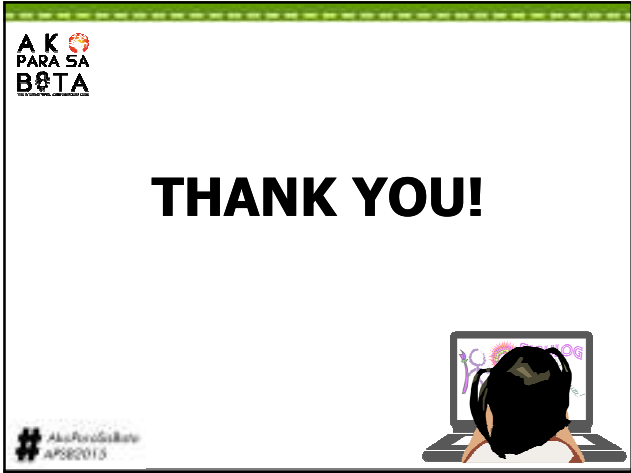
Open Forum

Summary



#AkParaSaBeta

APSE2013





Simultaneous Symposium 1: **Online Child Abuse (Part I): Definitions, Laws and Reporting, Initial Investigation**

Manila Room, 2nd level Marco Polo Plaza
1:30 – 5:00 PM


AkoParaSaBata
APSB2015



AK PARA SA BETA



ACP Robinson Landicho
*Republic Act No. 10175 (Cybercrime Prevention Act of 2012)
 and Related Special Laws*



Republic Act No. 10175
Cybercrime Prevention Act of 2012
and Related Special Laws

ACP ROBINSON A. LANDICHO
 OCP – Pasig City
 2 December 2015

AK PARA SA BETA
 THE INTERNATIONAL CONFERENCE IN CEBU

Special Laws

RA 10175 – Cybercrime Prevention Act of 2012

RA 9995 – Anti-Photo and Voyeurism Act of 2009

RA 9775 – Anti-Child Pornography Act of 2009

RA 9208 – Anti-Trafficking in Persons Act of 2003

RA 8792 – E-Commerce Act of 2000

RA 8484 – Access Devices Regulation Act of 1998

RA 7610 – Special Protection of Children Against Abuse,
 Exploitation and Discrimination Act

RA 4200 – Anti-Wiretapping Law of 1965

Supreme Court Rules on Electronic Evidence

AK PARA SA BETA
 THE INTERNATIONAL CONFERENCE IN CEBU

(a) Offenses against the confidentiality, integrity
 and availability of computer data and systems:

- (1) Illegal Access
- (2) Illegal Interception
- (3) Data Interference
- (4) System Interference
- (5) Misuse of Devices
- (6) Cyber-squatting

AK PARA SA BETA
 THE INTERNATIONAL CONFERENCE IN CEBU

Illegal access

covers the basic offence of dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data.

The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner.

Such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery.

"Access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data). However, it does not include the mere sending of an e-mail message or file to that system.

"Access" includes the entering of another computer system, where it is connected via public telecommunication networks, or to a computer system on the same network, such as a LAN (local area network) or Intranet within an organisation. The method of communication (e.g. from a distance, including via wireless links or at a close range) does not matter.

The act must also be committed 'without right'.

Illegal Interception

aims to protect the right of privacy of data communication

The right to privacy of correspondence

This represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons

This principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer

Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes.

The offence applies to 'non-public' transmissions of computer data. The term 'non-public' qualifies the nature of the transmission (communication) process and not the nature of the data transmitted. The data communicated may be publicly available information, but the parties wish to communicate confidentially. Or data may be kept secret for commercial purposes until the service is paid, as in Pay-TV.

For criminal liability to attach, the illegal interception must be committed "intentionally", and "without right".

Data interference

The aim of this provision is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage. The protected legal interest here is the integrity and the proper functioning or use of stored computer data or computer programs.

'damaging' and 'deteriorating' as overlapping acts relate in particular to a negative alteration of the integrity or of information content of data and programmes.

'Deletion' of data is the equivalent of the destruction of a corporeal thing. It destroys them and makes them unrecognisable.

Suppressing of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored.

The term 'alteration' means the modification of existing data.

The above acts are only punishable if committed "without right". In addition, the offender must have acted "intentionally"

System interference

This is referred to as computer sabotage

The provision aims at criminalising the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data.

The protected legal interest is the interest of operators and users of computer or telecommunication systems being able to have them function properly.

The hindering must furthermore be "serious" in order to give rise to criminal sanction.

The hindering must be "without right".

The offence must be committed intentionally, that is the perpetrator must have the intent to seriously hinder.

Misuse of devices

This provision establishes as a separate and independent criminal offence the intentional commission of specific illegal acts regarding certain devices or access data to be misused for the purpose of committing the above-described offences against the confidentiality, the integrity and availability of computer systems or data.

'Distribution' refers to the active act of forwarding data to others, while 'making available' refers to the placing online devices for the use of others. This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices. The inclusion of a 'computer program' refers to programs that are for example designed to alter or even destroy data or interfere with the operation of systems, such as virus programs, or programs designed or adapted to gain access to computer systems.

The offence requires that it be committed intentionally and without right.

Cybersquatting

Also known as domain squatting

According to the United States federal law known as the Anticybersquatting Consumer Protection Act, Cybersquatting is the registering, trafficking in, or using an Internet Domain Name with bad faith intent to profit from the goodwill of a trademark belonging to someone else. The cybersquatter then offers to sell the domain to the person or company who owns a trademark contained within the name at an inflated price.

The term is derived from "Squatting", which is the act of occupying an abandoned or unoccupied space or building that the squatter does not own, rent, or otherwise have permission to use.

Cybersquatting, however, is a bit different in that the domain names that are being "squatted" are (sometimes but not always) being paid for through the registration process by the cybersquatters.

Cybersquatters sometimes register variants of popular trademarked names, a practice known as “Typosquatting.”

Cybersquatting may also be committed through Renewal Snatching, Extension Exaggeration, and Alert Angling

As when Internet domain name registrations are for a fixed period of time. If the owner of a domain name doesn't re-register the name with an internet registrar prior to the domain's expiration date, then the domain name can be purchased by anybody else after it expires. At this point the registration is considered *lapsed*. A cybersquatter may use automated software tools to register the lapsed name the instant it is lapsed.

A **domain name** is an identification “string” that defines a realm of administrative autonomy, authority or control within the Internet.

Domain names are formed by the rules and procedures of the Domain Name System (DNS).

Any name registered in the DNS is a domain name.

Domain names are used in various networking contexts and application-specific naming and addressing purposes.

In general, a domain name represents an Internet Protocol (IP) resource, such as a personal computer used to access the Internet, a server computer hosting a website, or the web site itself or any other service communicated via the Internet.

Domain names serve as names for Internet resources such as computers, networks, and services. A domain name represents an Internet Protocol (IP) resource. Individual Internet host computers use domain names as host identifiers, or host names. Host names are the leaf labels in the domain name system usually without further subordinate domain name space. Host names appear as a component in Uniform Resource Locators (URLs) for Internet resources such as websites (e.g., en.wikipedia.org).

Domain names are also used as simple identification labels to indicate ownership or control of a resource. Such examples are the realm identifiers used in the Session Initiation Protocol (SIP), the Domain Keys used to verify DNS domains in e-mail systems, and in many other Uniform Resource Identifiers (URIs).

An important function of domain names is to provide easily recognizable and memorable names to numerically addressed Internet resources. This abstraction allows any resource to be moved to a different physical location in the address topology of the network, globally or locally in an intranet. Such a move usually requires changing the IP address of a resource and the corresponding translation of this IP address to and from its domain name.

Domain names are used to establish a unique identity. Organizations can choose a domain name that corresponds to their name, helping Internet users to reach them easily.

Domain names are often simply referred to as *domains* and domain name registrants are frequently referred to as *domain owners*, although domain name registration with a registrar does not confer any legal ownership of the domain name, only an exclusive right of use for a particular duration of time. The use of domain names in commerce may subject them to trademark law.

Panavision Int'l, L.P. v. Toeppen
141 F.3d 1316 (9th Cir. 1998), aff'g 945 F.
Supp. 1296 (C.D. Cal. 1996)

(b) Computer-related Offenses:

- (1) Computer-related Forgery
- (2) Computer-related Fraud
- (3) Computer-related Identity Theft

(c) Content-related Offenses:

- (1) Cybersex
- (2) Child Pornography
- (3) Unsolicited Commercial Communications
- (4) Libel (only with respect to the original author of the post)

SEC. 5. *Other Offenses*

(a) Aiding or Abetting in the Commission of Cybercrime

(b) Attempt in the Commission of Cybercrime

[does not apply to child pornography under Section 4 (c) (2); unsolicited commercial communications under Section 4 (c) (3); on-line libel under Section 4 (c) (4)]

SEC. 6. All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, **if committed by, through and with the use of information and communications technologies** shall be covered by the relevant provisions of this Act: *Provided*, That the **penalty to be imposed shall be one (1) degree higher** than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

SEC. 7. *Liability under Other Laws.* — A prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws. **[except prosecution of an offender under both Section (c) (4) (on-line libel) and Article 353 of the RPC (libel); and also where it pertains to Section 4 (c) (2) (child pornography) for being in violation of the prohibition against double jeopardy]**

SEC. 9. *Corporate Liability.* — When any of the punishable acts herein defined are **knowingly committed on behalf of or for the benefit of a juridical person, by a natural person acting either individually or as part of an organ of the juridical person, who has a leading position within, based on:**

(a) a power of representation of the juridical person provided the act committed falls within the scope of such authority;

(b) an authority to take decisions on behalf of the juridical person: *Provided*, That the act committed falls within the scope of such authority; or

(c) an authority to exercise control within the juridical person, **the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Ten million pesos (PhP10,000,000.00).**

If the commission of any of the punishable acts herein defined was made possible due to the lack of supervision or control by a natural person referred to and described in the preceding paragraph, for the benefit of that juridical person by a natural person acting under its authority, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Five million pesos (PhP5,000,000.00).

The liability imposed on the juridical person shall be without prejudice to the criminal liability of the natural person who has committed the offense.

SEC. 10. *Law Enforcement Authorities.* —

The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The NBI and the PNP shall organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations of this Act.

SEC. 11. *Duties of Law Enforcement Authorities.*

— To ensure that the technical nature of cybercrime and its prevention is given focus and considering the procedures involved for international cooperation, law enforcement authorities specifically the computer or technology crime divisions or units responsible for the investigation of cybercrimes are required to submit timely and regular reports including pre-operation, post-operation and investigation results and such other documents as may be required to the Department of Justice (DOJ) for review and monitoring.

SEC. 13. *Preservation of Computer Data.* —

The integrity of traffic data and subscriber information relating to communication services provided by a service provider shall be preserved for a minimum period of six (6) months from the date of the transaction.

Content data shall be similarly preserved for six (6) months from the date of receipt of the order from law enforcement authorities requiring its preservation.

Law enforcement authorities may order a one time extension for another six (6) months:

Provided, That once computer data preserved, transmitted or stored by a service provider is used as evidence in a case, the mere furnishing to such service provider of the transmittal document to the Office of the Prosecutor shall be deemed a notification to preserve the computer data until the termination of the case.

The service provider ordered to preserve computer data shall keep confidential the order and its compliance.

SEC. 14. *Disclosure of Computer Data.* —

Law enforcement authorities, **upon securing a court warrant**, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation.

SEC. 15. *Search, Seizure and Examination of Computer Data.* —

Where a search and seizure warrant is properly issued, the law enforcement authorities shall likewise have the following powers and duties.

Within the time period specified in the warrant, to conduct interception, as defined in this Act, and:

- (a) To secure a computer system or a computer data storage medium;
- (b) To make and retain a copy of those computer data secured;
- (c) To maintain the integrity of the relevant stored computer data;

- (d) **To conduct forensic analysis or examination of the computer data storage medium; and**
- (e) To render inaccessible or remove those computer data in the accessed computer or computer and communications network.

Pursuant thereof, the law enforcement authorities may order any person who has knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the search, seizure and examination.

Law enforcement authorities may request for an extension of time to complete the examination of the computer data storage medium and to make a return thereon but in no case for a period longer than thirty (30) days from date of approval by the court.

SEC. 16. Custody of Computer Data.

All computer data, including content and traffic data, examined under a proper warrant shall, within forty-eight (48) hours after the expiration of the period fixed therein, be deposited with the court in a sealed package,

and shall be accompanied by an affidavit of the law enforcement authority executing it stating the dates and times covered by the examination, and the law enforcement authority who may access the deposit, among other relevant data.

The law enforcement authority **shall also certify** that no duplicates or copies of the whole or any part thereof have been made, or if made, that all such duplicates or copies are included in the package deposited with the court.

The package so deposited shall not be opened, or the recordings replayed, or used in evidence, or then contents revealed, **except upon order of the court, which shall not be granted except upon motion, with due notice and opportunity to be heard to the person or persons whose conversation or communications have been recorded.**

SEC. 17. *Destruction of Computer Data.* —

Upon expiration of the periods as provided in Sections 13 and 15, service providers and law enforcement authorities, as the case may be, **shall immediately and completely destroy the computer data subject of a preservation and examination.**

SEC. 18. *Exclusionary Rule.* —

Any evidence procured without a valid warrant or beyond the authority of the same shall be inadmissible for any proceeding before any court or tribunal.

SEC. 20. *Noncompliance.* — Failure to comply with the provisions of Chapter IV hereof specifically the orders from law enforcement authorities shall be punished as a violation of Presidential Decree No. 1829 with imprisonment of *prison correctional* in its maximum period or a fine of One hundred thousand pesos (Php100,000.00) or both, for each and every noncompliance with an order issued by law enforcement authorities.

SEC. 21. *Jurisdiction.* — The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act, including any violation committed by a Filipino national regardless of the place of commission.

Jurisdiction shall lie if any of the elements was committed within the Philippines

or committed with the use of any computer system wholly or partly situated in the country,

or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.

There shall be designated special cybercrime courts manned by specially trained judges to handle cybercrime cases.

**Republic Act No. 10175
Cybercrime Prevention Act of 2012**

Cyber Crime Offences:

(1) Cybersex - willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.

(2) Child Pornography — The unlawful or prohibited acts defined and punishable by the Anti-Child Pornography Act of 2009, committed through a computer system.

**Republic Act No. 9775
Anti-Child Pornographic Act of 2009**

Child Pornography - any representation, whether visual, audio, or written combination thereof, by **electronic**, mechanical, digital, optical, magnetic or any other means, of child engaged or involved in real or simulated explicit sexual activities.

AKO PARA SA BOTA
THE INTERNATIONAL CONFERENCE IN CEBU

Duties of Internet Content Host :

- (a) Not host any form of child pornography on its internet address;
- (b) Within 7 days, report the presence of any form of child pornography
- (c) Preserve such evidence

AKO PARA SA BOTA
THE INTERNATIONAL CONFERENCE IN CEBU

**Republic Act No. 9775
Anti-Child Pornographic Act of 2009**

Authority of the LGU of the city or municipality where an internet café or kiosk is located to monitor and regulate the establishment and operation of the same or similar establishments.

Inter - Agency Council Against Child Pornography composed of the different government and non-government agencies

AKO PARA SA BOTA
THE INTERNATIONAL CONFERENCE IN CEBU

**Republic Act No. 9995
Anti-Photo and Video Voyeurism Act of 2009**

Photo or video voyeurism as the means the act of taking photo or video coverage of a person or group of persons performing sexual act or any similar activity or of capturing an image of the private area of a person or persons without the latter's consent

AKO PARA SA BOTA
THE INTERNATIONAL CONFERENCE IN CEBU

**Republic Act No. 9995
Anti-Photo and Video Voyeurism Act of 2009**

Prohibited Acts:

- (a) To take photo or video coverage of a person or group of persons performing sexual act or any similar activity or to capture an image of the private area of a without the consent of the person/s involved and under circumstances in which the person/s has/have a reasonable expectation of privacy;

**Republic Act No. 9995
Anti-Photo and Video Voyeurism Act of 2009**

Prohibited Acts

- (b) To copy or reproduce, or to cause to be copied or reproduced, such photo or video or recording of sexual act or any similar activity with or without consideration;

- (c) To sell or distribute, or cause to be sold or distributed, such photo or video or recording of sexual act, whether it be the original copy or reproduction thereof; or

- (d) To publish or broadcast, or cause to be published or broadcast, whether in print or broadcast media, or show or exhibit the photo or video coverage or recordings of such sexual act or any similar activity through VCD/DVD, internet, cellular phones and other similar means or device.

**Republic Act No. 9208
Anti-Trafficking in Persons Act of 2003**

Pornography - any representation, through publication, exhibition, cinematography, indecent shows, information technology, or by whatever means, of a person engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a person for primarily sexual purposes.

Prostitution - any act, transaction, scheme or design involving the use of a person by another, for sexual intercourse or lascivious conduct in exchange for money, profit or any other consideration.

**Republic Act No. 8792
E-Commerce Act**

Provides for the admissibility of electronic evidence in the courts of law, subject to certain conditions

Treats hacking, introduction of viruses and copyright violations as crimes

Promotes utilization of online commerce in the country and provides certain safeguards

Reduce graft and corruption in government as it lessens personal interaction between government agents and private individuals

Section 12. Admissibility and Evidential Weight of Electronic Data Message or Electronic Document. - In any legal proceedings, nothing in the application of the rules on evidence shall deny the admissibility of an electronic data message or electronic document in evidence -

(a) On the sole ground that it is in electronic form;

Or (b) On the ground that it is not in the standard written form, and the electronic data message or electronic document meeting, and complying with the requirements under Sections 6 or 7 hereof shall be the best evidence of the agreement and transaction contained therein. (RA 8792)

In assessing the evidential weight of an electronic data message or electronic document, the reliability of the manner in which it was generated, stored or communicated, the reliability of the manner in which its originator was identified, and other relevant factors shall be given due regard.

Republic Act No. 8484
Access Device Regulation Act of 1998

Regulates use of access devices, prohibiting fraudulent acts committed and providing penalties

Prohibited Acts:

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

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

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

(d) using an access device fraudulently applied for;

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

X X X X X X

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

Republic Act No. 7610
Special Protection of Children Against Abuse, Exploitation and Discrimination Act

Punishable Acts:

Section 5. Child Prostitution and Other Sexual Abuse.

Section 6. Attempt To Commit Child Prostitution.

Section 7. Child Trafficking.

Section 8. Attempt to Commit Child Trafficking.

Section 9. Obscene Publications and Indecent Shows

Section 10. Other Acts of Neglect, Abuse, Cruelty or Exploitation and Other Conditions Prejudicial to the Child's Development

Section 11. Sanctions of Establishments or Enterprises which Promote, Facilitate, or Conduct Activities Constituting Child Prostitution and Other Sexual Abuse, Child Trafficking, Obscene Publications and Indecent Shows, and Other Acts of Abuse

**Republic Act No. 4200
Anti-Wire Tapping Act of 1965**

Section 1. It shall be unlawful for any person, not being authorized by all the parties to any private communication or spoken word, to tap any wire or cable, or by using any other device or arrangement, to secretly overhear, intercept, or record such communication or spoken word by using a device commonly known as a dictaphone or dictagraph or dictaphone or walkie-talkie or tape recorder, or *however otherwise described*

**Philippine Supreme Court Rule on
Electronic Evidence**

Rules on the admissibility and reliability of electronic evidence

A.M. NO. 01-7-01-SC.- RE: RULES ON ELECTRONIC EVIDENCE

SEC. 2. *Cases covered.* - These Rules shall apply to all civil actions and proceedings, as well as quasi-judicial and administrative cases.

Philippine Supreme Court Rule on Electronic Evidence

(g) “*Electronic data message*” refers to information generated, sent, received or stored by electronic, optical or similar means.

(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”.

Philippine Supreme Court Rule on Electronic Evidence

MCC **INDUSTRIAL** **SALES**
CORPORATION **VS.** **SSANGYONG**
CORPORATION October 17, 2007 G.R.
No. 170633

Whether the print-out and/or photocopies of facsimile transmissions are electronic evidence and admissible as such?

Facsimile transmissions are not, in this sense, “paperless,” but verily are paper-based.

Philippine Supreme Court Rule on Electronic Evidence

Accordingly, in an ordinary facsimile transmission, there exists an original *paper-based* information or data that is scanned, sent through a phone line, and re-printed at the receiving end.

Be it noted that in enacting the Electronic Commerce Act of 2000, Congress intended *virtual or paperless* writings to be the *functional* equivalent and to have the same *legal function* as paper-based documents.

Further, in a virtual or paperless environment, technically, there is no original copy to speak of, as all direct printouts of the virtual reality are the same, in all respects, and are considered as originals.

Philippine Supreme Court Rule on Electronic Evidence

Ineluctably, the law's definition of "electronic data message," which, as aforesaid, is interchangeable with "electronic document," could not have included *facsimile transmissions*, which have an *original paper-based copy as sent* and a *paper-based facsimile copy as received*. These two copies are distinct from each other, and have different legal effects.

While Congress anticipated future developments in communications and computer technology when it drafted the law, it excluded the early forms of technology, like telegraph, telex and telecopy (except computer-generated faxes, which is a newer development as compared to the ordinary fax machine to fax machine transmission), when it defined the term "electronic data message."

Philippine Supreme Court Rule on Electronic Evidence

NATIONAL POWER CORPORATION VS. HON. RAMON G. CODILLA, JR., Presiding Judge, RTC of Cebu, Br. 19, BANGPAI SHIPPING COMPANY, and WALLEM SHIPPING, INCORPORATED
G.R. No. 170491, April 4, 2007

The focal point of this entire controversy is petitioner's obstinate contention that the photocopies it offered as formal evidence before the trial court are the functional equivalent of their original based on its inimitable interpretation of the Rules on Electronic Evidence.

Philippine Supreme Court Rule on Electronic Evidence

“electronic document” refers to **information or the representation of information, data, figures, symbols or other models 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.**

Hence, the argument of petitioner that since these paper printouts were produced through an electronic process, then these photocopies are electronic documents as defined in the Rules on Electronic Evidence is obviously an erroneous, if not preposterous, interpretation of the law.

Philippine Supreme Court Rule on Electronic Evidence

RUSTAN ANG y PASCUA VS. THE HONORABLE COURT OF APPEALS and IRISH SAGUD G.R. No. 182835 April 20, 2010

“Besides, the rules he 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.”

**Philippine Supreme Court Rule on
Electronic Evidence**

EN BANC

A.M. No. 01-7-01-SC

**RE: EXPANSION OF THE COVERAGE OF
THE RULES ON ELECTRONIC
EVIDENCE**

AKO PARA SA BOTA
THE INTERNATIONAL CONFERENCE IN CEBU

RESOLUTION

Acting on the letter of the Chairman of the Committee on Revision of the Rules of Court, the Court Resolved to AMEND Section 2, Rule 1 of the Rules on Electronic Evidence to read as follows:

AKO PARA SA BOTA
THE INTERNATIONAL CONFERENCE IN CEBU

**Philippine Supreme Court Rule on
Electronic Evidence**

"SEC. 2 Cases covered. - These Rules shall apply to the criminal and civil actions and proceeding, as well as quasi-judicial and administrative cases."

AKO PARA SA BOTA
THE INTERNATIONAL CONFERENCE IN CEBU

The amendment shall take effect on October 14, 2002 following the publication of this Resolution in a newspaper of general circulation.

September 24, 2002.

AKO PARA SA BOTA
THE INTERNATIONAL CONFERENCE IN CEBU

People Vs. Enojas, Et al., G.R. No. 204894, March 10, 2014. Abad, J.

As to the admissibility of the text messages, the RTC admitted them in conformity with the Court's earlier Resolution applying the Rules on Electronic Evidence to criminal actions (citing A.M. No. 01-7-01-SC, Re: Expansion of the Coverage of the Rules on Electronic Evidence, September 24, 2002)

AKO PARA SA BOTA
THE INTERNATIONAL CONFERENCE IN CEBU


Child Protection Network with **ENERGEN** and **unicef** present

AKO PARA SA BOTA
THE INTERNATIONAL CONFERENCE IN CEBU

Theme:
CYBERPROTECTION OF CHILDREN

Cyber Safety of Children:
Internet and Mobile Protection for Minors

#AkoParaSaBota
APSC2013



Republic Act No. 9775

otherwise known as the

“Anti-Child Pornography Act of 2009”

“Child” refers to a person below eighteen (18) years of age or over, but is unable to fully take care of himself/herself from abuse, neglect, cruelty, exploitation or discrimination because of a physical or mental disability or condition.

Child shall also refer to:

(1) a person regardless of age who is presented, depicted or portrayed as a child as defined herein; and

(2) computer-generated, digitally or manually crafted images or graphics of a person who is represented or who is made to appear to be a child as defined herein.

“Child pornography” refers to any representation, whether visual, audio, or written combination thereof, by electronic, mechanical, digital, optical, magnetic or any other means, of child engaged or involved in real or simulated explicit sexual activities.

“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

Unlawful or Prohibited Acts.

- (a) To hire, employ, use, persuade, induce or coerce a child to perform in the creation or production of any form of child pornography

- (b) To produce, direct, manufacture or create any form of child pornography
- (c) To publish offer, transmit, sell, distribute, broadcast, advertise, promote, export or import any form of child pornography

- (d) To possess any form of child pornography with the intent to sell, distribute, publish, or broadcast:

Provided: That possession of three (3) or more articles of child pornography of the same form shall be prima facie evidence of the intent to sell, distribute, publish or broadcast

(e) To knowingly, willfully and intentionally provide a venue for the commission of prohibited acts as, but not limited to, dens, private rooms, cubicles, cinemas, houses or in establishments purporting to be a legitimate business

(f) For film distributors, theaters and telecommunication companies, by themselves or in cooperation with other entities, to distribute any form of child pornography

(g) For a parent, legal guardian or person having custody or control of a child to knowingly permit the child to engage, participate or assist in any form of child pornography

(h) To engage in the luring or grooming of a child

“Grooming” refers to the act of preparing a child or someone who the offender believes to be a child for sexual activity or sexual relationship by communicating any form of child pornography. It includes online enticement or enticement through any other means.

“Luring” refers to the act of communicating, by means of a computer system, with a child or someone who the offender believes to be a child for the purpose of facilitating the commission of sexual activity or production of any form of child pornography.

(i) To engage in pandering of any form of child pornography

“Pandering” refers to the act of offering, advertising, promoting, representing or distributing through any means any material or purported material that is intended to cause another to believe that the material or purported material contains any form of child pornography, regardless of the actual content of the material or purported material

(j) To willfully access any form of child pornography

(k) To conspire to commit any of the prohibited acts stated in this section. Conspiracy to commit any form of child pornography shall be committed when two (2) or more persons come to an agreement concerning the commission of any of the said prohibited acts and decide to commit it

(l) To possess any form of child pornography

Syndicated Child Pornography – The crime of child pornography is deemed committed by a syndicate if carried out by a group of three (3) or more persons conspiring or confederating with one another

Who May File a Complaint

- (a) Offended party;
- (b) Parents or guardians;
- (c) Ascendant or collateral relative within the third degree of consanguinity;

(d) Officer, social worker or representative of a licensed child-caring institution;

(e) Officer or social worker of the Department of Social Welfare and Development (DSWD);

(f) Local social welfare development officer;

(g) Barangay Chairman;

(h) Any law enforcement officer;

(i) At least three (3) concerned responsible citizens residing in the place where the violation occurred;

(j) Any person who has personal knowledge of the circumstances of the commission of any offense under this Act.

The Department of Justice (DOJ) shall appoint or designate special prosecutors to prosecute cases for the violation of this Act.

Jurisdiction over cases for the violation of this Act shall be vested in the Family Court which has territorial jurisdiction over the place where the offense or any of its essential elements was committed

All internet service providers (ISPs) shall notify the Philippine National Police (PNP) or the National Bureau of Investigation (NBI) within seven (7) days from obtaining facts and circumstances that any form of child pornography is being committed using its server or facility.

All mall owners/operators and owners or lessors of other business establishments shall notify the PNP or the NBI within seven (7) days from obtaining facts and circumstances that child pornography is being committed in their premises.

Public display of any form of child pornography within their premises is a conclusive presumption of the knowledge of the mall owners/operators and owners or lessors of other business establishments of the violation of this Act

A disputable presumption of knowledge by mall owners/operators and owners or lessors of other business establishments should know or reasonably know that a violation of this Act is being committed in their premises

Photo developers, information technology professionals, credit card companies and banks and any person who has direct knowledge of any form of child pornography activities shall have the duty to report any suspected child pornography materials or transactions to the proper authorities within seven (7) days from discovery thereof.

Duties of an Internet Content Host:

(a) Not host any form of child pornography on its internet address;

(b) Within seven (7) days, report the presence of any form of child pornography, as well as the particulars of the person maintaining, hosting, distributing or in any manner contributing to such internet address, to the proper authorities; and

(c) Preserve such evidence for purposes of investigation and prosecution by relevant authorities.

An internet content host shall, upon the request of proper authorities, furnish the particulars of users who gained or attempted to gain access to an internet address that contains any form of child pornography.

That the failure of the internet content host to remove any form of child pornography within forty-eight (48) hours from receiving the notice that any form of child pornography is hitting its server shall be conclusive evidence of willful and intentional violation thereof

The local government unit (LGU) of the city or municipality where an internet café or kiosk is located shall have the authority to monitor and regulate the establishment and operation of the same or similar establishments in order to prevent violation of the provisions of this Act.

The right to privacy of the child shall be ensured at any stage of the investigation, prosecution and trial of an offense under this Act.

If the offender is a parent, ascendant, guardian, step-parent or collateral relative within the third degree of consanguinity or affinity or any person having control or moral ascendancy over the child, the penalty provided herein shall be in its maximum duration

If the offender is a juridical person, the penalty shall be imposed upon the owner, manager, partner, member of the board of directors and/or any responsible officer who participated in the commission of the crime or shall have knowingly permitted or failed to prevent its commissions

If the offender is a foreigner, he/she shall be immediately deported after the complete service of his/her sentence and shall forever be barred from entering the country

The penalty provided for in this Act shall be imposed in its maximum duration if the offender is a public officer or employee

Pursuant to the Convention on Transnational Organized Crime, the DOJ may execute the request of a foreign state for assistance in the investigation or prosecution of any form of child pornography by:

- (1) conducting a preliminary investigation against the offender and, if appropriate, to file the necessary charges in court;
- (2) giving information needed by the foreign state;

- (3) to apply for an order of forfeiture of any proceeds or monetary instrument or properly located in the Philippines used in connection with child pornography in the court

The principles of mutuality and reciprocity shall, for this purpose, be at all times recognized

The DOJ, in consultation with the Department of Foreign Affairs (DFA), shall endeavor to include child pornography among extraditable offenses in future treaties.

The Revised penal Code shall be
suppletorily applicable to this Act



Republic Act No. 10175 Cybercrime Prevention Act of 2012 and Related Special Laws

ACP ROBINSON A. LANDICHO
OCP – Pasig City
2 December 2015

Special Laws

RA 10175 – Cybercrime Prevention Act of 2012

RA 9995 – Anti-Photo and Voyeurism Act of 2009

RA 9775 – Anti-Child Pornography Act of 2009

RA 9208 – Anti-Trafficking in Persons Act of 2003

RA 8792 – E-Commerce Act of 2000

RA 8484 – Access Devices Regulation Act of 1998

RA 7610 – Special Protection of Children Against Abuse,
Exploitation and Discrimination Act

RA 4200 – Anti-Wiretapping Law of 1965

Supreme Court Rules on Electronic Evidence

(a) Offenses against the confidentiality, integrity and availability of computer data and systems:

- (1) Illegal Access
- (2) Illegal Interception
- (3) Data Interference
- (4) System Interference
- (5) Misuse of Devices
- (6) Cyber-squatting

Illegal access

covers the basic offence of dangerous threats to and attacks against the security (i.e. the confidentiality, integrity and availability) of computer systems and data.

The need for protection reflects the interests of organisations and individuals to manage, operate and control their systems in an undisturbed and uninhibited manner.

Such intrusions may give access to confidential data (including passwords, information about the targeted system) and secrets, to the use of the system without payment or even encourage hackers to commit more dangerous forms of computer-related offences, like computer-related fraud or forgery.

"Access" comprises the entering of the whole or any part of a computer system (hardware, components, stored data of the system installed, directories, traffic and content-related data). However, it does not include the mere sending of an e-mail message or file to that system.

"Access" includes the entering of another computer system, where it is connected via public telecommunication networks, or to a computer system on the same network, such as a LAN (local area network) or Intranet within an organisation. The method of communication (e.g. from a distance, including via wireless links or at a close range) does not matter.

The act must also be committed 'without right'.

Illegal Interception

aims to protect the right of privacy of data communication

The right to privacy of correspondence

This represents the same violation of the privacy of communications as traditional tapping and recording of oral telephone conversations between persons

This principle to all forms of electronic data transfer, whether by telephone, fax, e-mail or file transfer

Interception by 'technical means' relates to listening to, monitoring or surveillance of the content of communications, to the procuring of the content of data either directly, through access and use of the computer system, or indirectly, through the use of electronic eavesdropping or tapping devices. Interception may also involve recording. Technical means includes technical devices fixed to transmission lines as well as devices to collect and record wireless communications. They may include the use of software, passwords and codes.

The offence applies to 'non-public' transmissions of computer data. The term 'non-public' qualifies the nature of the transmission (communication) process and not the nature of the data transmitted. The data communicated may be publicly available information, but the parties wish to communicate confidentially. Or data may be kept secret for commercial purposes until the service is paid, as in Pay-TV.

For criminal liability to attach, the illegal interception must be committed "intentionally", and "without right".

Data interference

The aim of this provision is to provide computer data and computer programs with protection similar to that enjoyed by corporeal objects against intentional infliction of damage. The protected legal interest here is the integrity and the proper functioning or use of stored computer data or computer programs.

'damaging' and 'deteriorating' as overlapping acts relate in particular to a negative alteration of the integrity or of information content of data and programmes.

'Deletion' of data is the equivalent of the destruction of a corporeal thing. It destroys them and makes them unrecognisable.

Suppressing of computer data means any action that prevents or terminates the availability of the data to the person who has access to the computer or the data carrier on which it was stored.

The term 'alteration' means the modification of existing data.

The above acts are only punishable if committed "without right". In addition, the offender must have acted "intentionally"

System interference

This is referred to as computer sabotage

The provision aims at criminalising the intentional hindering of the lawful use of computer systems including telecommunications facilities by using or influencing computer data.

The protected legal interest is the interest of operators and users of computer or telecommunication systems being able to have them function properly.

The hindering must furthermore be "serious" in order to give rise to criminal sanction.

The hindering must be "without right".

The offence must be committed intentionally, that is the perpetrator must have the intent to seriously hinder.

Misuse of devices

This provision establishes as a separate and independent criminal offence the intentional commission of specific illegal acts regarding certain devices or access data to be misused for the purpose of committing the above-described offences against the confidentiality, the integrity and availability of computer systems or data.

'Distribution' refers to the active act of forwarding data to others, while 'making available' refers to the placing online devices for the use of others. This term also intends to cover the creation or compilation of hyperlinks in order to facilitate access to such devices. The inclusion of a 'computer program' refers to programs that are for example designed to alter or even destroy data or interfere with the operation of systems, such as virus programs, or programs designed or adapted to gain access to computer systems.

The offence requires that it be committed intentionally and without right.

Cybersquatting

Also known as domain squatting

According to the United States federal law known as the Anticybersquatting Consumer Protection Act, Cybersquatting is the registering, trafficking in, or using an Internet Domain Name with bad faith intent to profit from the goodwill of a trademark belonging to someone else. The cybersquatter then offers to sell the domain to the person or company who owns a trademark contained within the name at an inflated price.

The term is derived from "Squatting", which is the act of occupying an abandoned or unoccupied space or building that the squatter does not own, rent, or otherwise have permission to use.

Cybersquatting, however, is a bit different in that the domain names that are being "squatted" are (sometimes but not always) being paid for through the registration process by the cybersquatters.

Cybersquatters sometimes register variants of popular trademarked names, a practice known as "Typosquatting."

Cybersquatting may also be committed through Renewal Snatching, Extension Exaggeration, and Alert Angling

As when Internet domain name registrations are for a fixed period of time. If the owner of a domain name doesn't re-register the name with an internet registrar prior to the domain's expiration date, then the domain name can be purchased by anybody else after it expires. At this point the registration is considered *lapsed*. A cybersquatter may use automated software tools to register the lapsed name the instant it is lapsed.

A **domain name** is an identification "string" that defines a realm of administrative autonomy, authority or control within the Internet.

Domain names are formed by the rules and procedures of the Domain Name System (DNS).

Any name registered in the DNS is a domain name.

Domain names are used in various networking contexts and application-specific naming and addressing purposes.

In general, a domain name represents an Internet Protocol (IP) resource, such as a personal computer used to access the Internet, a server computer hosting a website, or the web site itself or any other service communicated via the Internet.

Domain names serve as names for Internet resources such as computers, networks, and services. A domain name represents an Internet Protocol (IP) resource. Individual Internet host computers use domain names as host identifiers, or host names. Host names are the leaf labels in the domain name system usually without further subordinate domain name space. Host names appear as a component in Uniform Resource Locators (URLs) for Internet resources such as websites (e.g., en.wikipedia.org).

Domain names are also used as simple identification labels to indicate ownership or control of a resource. Such examples are the realm identifiers used in the Session Initiation Protocol (SIP), the Domain Keys used to verify DNS domains in e-mail systems, and in many other Uniform Resource Identifiers (URIs).

An important function of domain names is to provide easily recognizable and memorable names to numerically addressed Internet resources. This abstraction allows any resource to be moved to a different physical location in the address topology of the network, globally or locally in an intranet. Such a move usually requires changing the IP address of a resource and the corresponding translation of this IP address to and from its domain name.

Domain names are used to establish a unique identity. Organizations can choose a domain name that corresponds to their name, helping Internet users to reach them easily.

Domain names are often simply referred to as *domains* and domain name registrants are frequently referred to as *domain owners*, although domain name registration with a registrar does not confer any legal ownership of the domain name, only an exclusive right of use for a particular duration of time. The use of domain names in commerce may subject them to trademark law.

Panavision Int'l, L.P. v. Toeppen
141 F.3d 1316 (9th Cir. 1998), aff'g 945 F. Supp. 1296 (C.D. Cal. 1996)

(b) Computer-related Offenses:

- (1) Computer-related Forgery
- (2) Computer-related Fraud
- (3) Computer-related Identity Theft

(c) Content-related Offenses:

- (1) Cybersex
- (2) Child Pornography
- (3) Unsolicited Commercial Communications
- (4) Libel (only with respect to the original author of the post)

SEC. 5. *Other Offenses*

(a) Aiding or Abetting in the Commission of Cybercrime

(b) Attempt in the Commission of Cybercrime

[does not apply to child pornography under Section 4 (c) (2); unsolicited commercial communications under Section 4 (c) (3); on-line libel under Section 4 (c) (4)]

SEC. 6. All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of this Act: *Provided*, That the penalty to be imposed shall be one (1) degree higher than that provided for by the Revised Penal Code, as amended, and special laws, as the case may be.

SEC. 7. *Liability under Other Laws.* — A prosecution under this Act shall be without prejudice to any liability for violation of any provision of the Revised Penal Code, as amended, or special laws. [except prosecution of an offender under both Section (c) (4) (on-line libel) and Article 353 of the RPC (libel); and also where it pertains to Section 4 (c) (2) (child pornography) for being in violation of the prohibition against double jeopardy]

SEC. 9. *Corporate Liability.* — When any of the punishable acts herein defined are knowingly committed on behalf of or for the benefit of a juridical person, by a natural person acting either individually or as part of an organ of the juridical person, who has a leading position within, based on:

(a) a power of representation of the juridical person provided the act committed falls within the scope of such authority;

(b) an authority to take decisions on behalf of the juridical person: *Provided*, That the act committed falls within the scope of such authority; or

(c) an authority to exercise control within the juridical person, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Ten million pesos (PhP10,000,000.00).

If the commission of any of the punishable acts herein defined was made possible due to the lack of supervision or control by a natural person referred to and described in the preceding paragraph, for the benefit of that juridical person by a natural person acting under its authority, the juridical person shall be held liable for a fine equivalent to at least double the fines imposable in Section 7 up to a maximum of Five million pesos (PhP5,000,000.00).

The liability imposed on the juridical person shall be without prejudice to the criminal liability of the natural person who has committed the offense.

SEC. 10. *Law Enforcement Authorities.* —

The National Bureau of Investigation (NBI) and the Philippine National Police (PNP) shall be responsible for the efficient and effective law enforcement of the provisions of this Act. The NBI and the PNP shall organize a cybercrime unit or center manned by special investigators to exclusively handle cases involving violations of this Act.

SEC. 11. *Duties of Law Enforcement Authorities.*

— To ensure that the technical nature of cybercrime and its prevention is given focus and considering the procedures involved for international cooperation, law enforcement authorities specifically the computer or technology crime divisions or units responsible for the investigation of cybercrimes are required to submit timely and regular reports including pre-operation, post-operation and investigation results and such other documents as may be required to the Department of Justice (DOJ) for review and monitoring.

SEC. 13. *Preservation of Computer Data.* —

The integrity of traffic data and subscriber information relating to communication services provided by a service provider shall be preserved for a minimum period of six (6) months from the date of the transaction.

Content data shall be similarly preserved for six (6) months from the date of receipt of the order from law enforcement authorities requiring its preservation.

Law enforcement authorities may order a one time extension for another six (6) months:

Provided, That once computer data preserved, transmitted or stored by a service provider is used as evidence in a case, the mere furnishing to such service provider of the transmittal document to the Office of the Prosecutor shall be deemed a notification to preserve the computer data until the termination of the case.

The service provider ordered to preserve computer data shall keep confidential the order and its compliance.

SEC. 14. *Disclosure of Computer Data.* —

Law enforcement authorities, upon securing a court warrant, shall issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data or relevant data in his/its possession or control within seventy-two (72) hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation.

SEC. 15. *Search, Seizure and Examination of Computer Data.* —

Where a search and seizure warrant is properly issued, the law enforcement authorities shall likewise have the following powers and duties.

Within the time period specified in the warrant, to conduct interception, as defined in this Act, and:

- (a) To secure a computer system or a computer data storage medium;
- (b) To make and retain a copy of those computer data secured;
- (c) To maintain the integrity of the relevant stored computer data;

(d) To conduct forensic analysis or examination of the computer data storage medium; and

(e) To render inaccessible or remove those computer data in the accessed computer or computer and communications network.

Pursuant thereof, the law enforcement authorities may order any person who has knowledge about the functioning of the computer system and the measures to protect and preserve the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the search, seizure and examination.

Law enforcement authorities may request for an extension of time to complete the examination of the computer data storage medium and to make a return thereon but in no case for a period longer than thirty (30) days from date of approval by the court.

SEC. 16. *Custody of Computer Data.*

All computer data, including content and traffic data, examined under a proper warrant shall, **within forty-eight (48) hours after the expiration of the period fixed therein, be deposited with the court in a sealed package,**

and shall be **accompanied by an affidavit** of the law enforcement authority executing it **stating the dates and times covered by the examination, and the law enforcement authority who may access the deposit, among other relevant data.**

The law enforcement authority **shall also certify** that no duplicates or copies of the whole or any part thereof have been made, or if made, that all such duplicates or copies are included in the package deposited with the court.

The package so deposited shall not be opened, or the recordings replayed, or used in evidence, or then contents revealed, *except upon order of the court, which shall not be granted except upon motion, with due notice and opportunity to be heard to the person or persons whose conversation or communications have been recorded.*

SEC. 17. *Destruction of Computer Data.* —

Upon expiration of the periods as provided in Sections 13 and 15, service providers and law enforcement authorities, as the case may be, *shall immediately and completely destroy the computer data subject of a preservation and examination.*

SEC. 18. *Exclusionary Rule.* —

Any evidence procured without a valid warrant or beyond the authority of the same shall be inadmissible for any proceeding before any court or tribunal.

SEC. 20. *Noncompliance.* — Failure to comply with the provisions of Chapter IV hereof specifically the orders from law enforcement authorities shall be punished as a violation of Presidential Decree No. 1829 with imprisonment of *prision correctional* in its maximum period or a fine of One hundred thousand pesos (Php100,000.00) or both, for each and every noncompliance with an order issued by law enforcement authorities.

SEC. 21. *Jurisdiction.* — The Regional Trial Court shall have jurisdiction over any violation of the provisions of this Act, including any violation committed by a Filipino national regardless of the place of commission.

Jurisdiction shall lie if any of the elements was committed within the Philippines

or committed with the use of any computer system wholly or partly situated in the country,

or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines.

There shall be designated special cybercrime courts manned by specially trained judges to handle cybercrime cases.

**Republic Act No. 10175
Cybercrime Prevention Act of 2012**

Cyber Crime Offences:

(1) Cybersex - willful engagement, maintenance, control, or operation, directly or indirectly, of any lascivious exhibition of sexual organs or sexual activity, with the aid of a computer system, for favor or consideration.

(2) Child Pornography — The unlawful or prohibited acts defined and punishable by the Anti-Child Pornography Act of 2009, committed through a computer system.

**Republic Act No. 9775
Anti-Child Pornographic Act of 2009**

Child Pornography - any representation, whether visual, audio, or written combination thereof, by **electronic**, mechanical, digital, optical, magnetic or any other means, of child engaged or involved in real or simulated explicit sexual activities.

Duties of Internet Content Host :

- (a) Not host any form of child pornography on its internet address;
- (b) Within 7 days, report the presence of any form of child pornography
- (c) Preserve such evidence

Republic Act No. 9775
Anti-Child Pornographic Act of 2009

Authority of the LGU of the city or municipality where an internet café or kiosk is located to monitor and regulate the establishment and operation of the same or similar establishments.

Inter - Agency Council Against Child Pornography composed of the different government and non-government agencies

Republic Act No. 9995
Anti-Photo and Video Voyeurism Act of 2009

Photo or video voyeurism as the means the act of taking photo or video coverage of a person or group of persons performing sexual act or any similar activity or of capturing an image of the private area of a person or persons without the latter's consent

Republic Act No. 9995
Anti-Photo and Video Voyeurism Act of 2009

Prohibited Acts:

- (a) To take photo or video coverage of a person or group of persons performing sexual act or any similar activity or to capture an image of the private area of a without the consent of the person/s involved and under circumstances in which the person/s has/have a reasonable expectation of privacy;

**Republic Act No. 9995
Anti-Photo and Video Voyeurism Act of 2009**

Prohibited Acts

(b) To copy or reproduce, or to cause to be copied or reproduced, such photo or video or recording of sexual act or any similar activity with or without consideration;

(c) To sell or distribute, or cause to be sold or distributed, such photo or video or recording of sexual act, whether it be the original copy or reproduction thereof; or

(d) To publish or broadcast, or cause to be published or broadcast, whether in print or broadcast media, or show or exhibit the photo or video coverage or recordings of such sexual act or any similar activity through VCD/DVD, internet, cellular phones and other similar means or device.

**Republic Act No. 9208
Anti-Trafficking in Persons Act of 2003**

Pornography - any representation, through publication, exhibition, cinematography, indecent shows, information technology, or by whatever means, of a person engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a person for primarily sexual purposes.

Prostitution - any act, transaction, scheme or design involving the use of a person by another, for sexual intercourse or lascivious conduct in exchange for money, profit or any other consideration.

**Republic Act No. 8792
E-Commerce Act**

Provides for the admissibility of electronic evidence in the courts of law, subject to certain conditions

Treats hacking, introduction of viruses and copyright violations as crimes

Promotes utilization of online commerce in the country and provides certain safeguards

Reduce graft and corruption in government as it lessens personal interaction between government agents and private individuals

Section 12. *Admissibility and Evidential Weight of Electronic Data Message or Electronic Document.* - In any legal proceedings, nothing in the application of the rules on evidence shall deny the admissibility of an electronic data message or electronic document in evidence -

(a) On the sole ground that it is in electronic form;

Or (b) On the ground that it is not in the standard written form, and the electronic data message or electronic document meeting, and complying with the requirements under Sections 6 or 7 hereof shall be the best evidence of the agreement and transaction contained therein. (RA 8792)

In assessing the evidential weight of an electronic data message or electronic document, the reliability of the manner in which it was generated, stored or communicated, the reliability of the manner in which its originator was identified, and other relevant factors shall be given due regard.

Republic Act No. 8484
Access Device Regulation Act of 1998

Regulates use of access devices, prohibiting fraudulent acts committed and providing penalties

Prohibited Acts:

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

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

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

(d) using an access device fraudulently applied for;

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

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

Republic Act No. 7610
Special Protection of Children Against Abuse, Exploitation and Discrimination Act

Punishable Acts:

Section 5. Child Prostitution and Other Sexual Abuse.

Section 6. Attempt To Commit Child Prostitution.

Section 7. Child Trafficking.

Section 8. Attempt to Commit Child Trafficking.

Section 9. Obscene Publications and Indecent Shows

Section 10. Other Acts of Neglect, Abuse, Cruelty or Exploitation and Other Conditions Prejudicial to the Child's Development

Section 11. Sanctions of Establishments or Enterprises which Promote, Facilitate, or Conduct Activities Constituting Child Prostitution and Other Sexual Abuse, Child Trafficking, Obscene Publications and Indecent Shows, and Other Acts of Abuse

Republic Act No. 4200 Anti-Wire Tapping Act of 1965

Section 1. It shall be unlawful for any person, not being authorized by all the parties to any private communication or spoken word, to tap any wire or cable, or by using any other device or arrangement, to secretly overhear, intercept, or record such communication or spoken word by using a device commonly known as a dictaphone or dictagraph or dictaphone or walkie-talkie or tape recorder, or *however otherwise described*

Philippine Supreme Court Rule on Electronic Evidence

Rules on the admissibility and reliability of electronic evidence

A.M. NO. 01-7-01-SC.- RE: RULES ON ELECTRONIC EVIDENCE

SEC. 2. *Cases covered.* - These Rules shall apply to all civil actions and proceedings, as well as quasi-judicial and administrative cases.

Philippine Supreme Court Rule on Electronic Evidence

(g) “*Electronic data message*” refers to information generated, sent, received or stored by electronic, optical or similar means.

(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”.

Philippine Supreme Court Rule on Electronic Evidence

**MCC INDUSTRIAL SALES
CORPORATION VS. SSANGYONG
CORPORATION** October 17, 2007 G.R.
No. 170633

Whether the print-out and/or photocopies of facsimile transmissions are electronic evidence and admissible as such?

Facsimile transmissions are not, in this sense, “paperless,” but verily are paper-based.

Philippine Supreme Court Rule on Electronic Evidence

Accordingly, in an ordinary facsimile transmission, there exists an original *paper-based* information or data that is scanned, sent through a phone line, and re-printed at the receiving end.

Be it noted that in enacting the Electronic Commerce Act of 2000, Congress intended *virtual or paperless* writings to be the *functional* equivalent and to have the same *legal function* as paper-based documents.

Further, in a virtual or paperless environment, technically, there is no original copy to speak of, as all direct printouts of the virtual reality are the same, in all respects, and are considered as originals.

Philippine Supreme Court Rule on Electronic Evidence

Ineluctably, the law's definition of "electronic data message," which, as aforesaid, is interchangeable with "electronic document," could not have included *facsimile transmissions*, which have an *original paper-based* copy *as sent* and a *paper-based facsimile* copy *as received*. These two copies are distinct from each other, and have different legal effects.

While Congress anticipated future developments in communications and computer technology when it drafted the law, it excluded the early forms of technology, like telegraph, telex and telecopy (except computer-generated faxes, which is a newer development as compared to the ordinary fax machine to fax machine transmission), when it defined the term “electronic data message.”

Philippine Supreme Court Rule on Electronic Evidence

NATIONAL POWER CORPORATION VS. HON. RAMON G. CODILLA, JR.,
Presiding Judge, RTC of Cebu, Br. 19,
BANGPAI SHIPPING COMPANY, and
WALLEM SHIPPING, INCORPORATED
G.R. No. 170491, April 4, 2007

The focal point of this entire controversy is petitioner's obstinate contention that the photocopies it offered as formal evidence before the trial court are the functional equivalent of their original based on its inimitable interpretation of the Rules on Electronic Evidence.

Philippine Supreme Court Rule on Electronic Evidence

“electronic document” refers to **information or the representation of information, data, figures, symbols or other models 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.**

Hence, the argument of petitioner that since these paper printouts were produced through an electronic process, then these photocopies are electronic documents as defined in the Rules on Electronic Evidence is obviously an erroneous, if not preposterous, interpretation of the law.

**Philippine Supreme Court Rule on
Electronic Evidence**

**RUSTAN ANG y PASCUA VS. THE
HONORABLE COURT OF APPEALS
and IRISH SAGUD G.R. No. 182835 April
20, 2010**

“Besides, the rules he 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.”

**Philippine Supreme Court Rule on
Electronic Evidence**

**EN BANC
A.M. No. 01-7-01-SC
RE: EXPANSION OF THE COVERAGE OF
THE RULES ON ELECTRONIC
EVIDENCE**

RESOLUTION

Acting on the letter of the Chairman of the Committee on Revision of the Rules of Court, the Court Resolved to AMEND Section 2, Rule 1 of the Rules on Electronic Evidence to read as follows:

Philippine Supreme Court Rule on Electronic Evidence

"SEC. 2 Cases covered. - These Rules shall apply to the criminal and civil actions and proceeding, as well as quasi-judicial and administrative cases."

The amendment shall take effect on October 14, 2002 following the publication of this Resolution in a newspaper of general circulation.

September 24, 2002.

People Vs. Enojas, Et al., G.R. No. 204894, March 10, 2014. Abad, J.

As to the **admissibility of the text messages**, the RTC admitted them **in conformity with the Court's earlier Resolution applying the Rules on Electronic Evidence to criminal actions** (citing A.M. No. 01-7-01-SC, Re: Expansion of the Coverage of the Rules on Electronic Evidence, September 24, 2002)

DOJ Media Guide

PRINCIPLES & GUIDE

Principle 1

Children have an absolute right to privacy. The highest ethical and professional standards in reporting and covering cases of children must be observed such that in all publicity concerning children, the best interests of the child shall be the primary concern.

Guide

1. In the best interest of the child, the identity of a child victim of abuse, child witness, CIAC or a CICL shall not be disclosed whether directly or indirectly.

No information that would lead to the identity of the child or any member of his/her family shall be published or broadcast.

2. Photographs, images, or video footage of the face or any distinguishing feature or information of a child victim of abuse, child witness, CIAC or a child in conflict with the law including his or her family members shall not be taken, published, or shown to the public in any manner.

Exception to this are missing children, children looking for their parents or relatives or any other similar cases where revealing the identify, is for the best interest of the child.

3. The disclosure of any private or graphic detail of the case, including the medico-legal findings, in public, is a violation of confidentiality provisions under the law.

4. The access, use or dissemination as well as the provision of records of a child shall be subject to sanctions under existing laws. Records, materials and other evidence recovered or confiscated during rescue operations of child victims are considered confidential when they form part of police, prosecution or court records.

5. In the best interest of the child, interview(s) of a child victim of abuse, child witness, child involved in armed conflict and a child in conflict with the law should be conducted only when the child interviewee is assisted by a psychologist or a social worker known to her or him. In this case, the media practitioner should take into consideration the level of comfort of the child when asking questions and the length of time spent in the interview. This is to prevent the child from further traumatising or victimization.

6. In reporting or covering cases on abuse and exploitation involving children, media practitioners are encouraged to discuss the issues surrounding the case rather than the personal circumstances of the victim.

Principle 2

The child's dignity must be respected at all times.

Guide

1. The use of sexualized images of children is a violation of the child's rights. Obscene or pornographic materials, videos, photographs and other related media should not be subjects of circulation, publication or broadcast as it is a violation of the right of the child to dignity and self-worth.

2. Crimes of violence by or against children must be reported factually and seriously without passing judgment, stereotyping, or sensationalism.

3. There should be a conscious effort to avoid sensationalism and exploitation of the child in need of any assistance. The release of the child's identity to elicit financial support or aid for the child's medical care is strongly discouraged.

4. The personal circumstance of the child which will tend to sensationalize the case must be avoided. The child's life should not be treated as a movie.

Principle 3

Children have the right to be heard.
Access to media by children should
be encouraged.

Guide

1. Whenever possible, give children access to media for them to be able to express their own opinions without inducement of any kind, in any manner or procedure affecting them.

2. When the child is the source of crime-related news or information, his/her identity should be protected at all times.

Principle 4

The mass media is a partner in the promotion of child rights and the prevention of child delinquency, and is encouraged to relay consistent messages through a balanced approach.

Journalistic activity which touches on the lives and welfare of children must be carried out with sensitivity and appreciation of the vulnerable situation of children, so that children are not re-victimized or re-traumatized.

Guide

1. On media coverage of specific cases, the present as well as the long-term implications for the child's recovery, rehabilitation and reintegration shall be taken into consideration by all those involved in deciding on and implementing the said approaches to media coverage.

2. It is the responsibility of the media to verify the status of an organization which purports to speak or represent the child, before any airing, broadcasting or publication in behalf of the child. The organization must be duly accredited, registered or licensed by the Department of Social Welfare and Development (DSWD) or by any appropriate government agency.

3. Media is urged to undertake investigative journalism and to report on violations of children's rights, and other issues relating to children's safety, privacy, security, education, health and social welfare and all forms of exploitation and discrimination.

4. xxx Media organizations are urged to develop their own internal policies and procedures aligned and consistent with these guidelines, including monitoring systems and protection mechanisms on the engagement of children in any media program to ensure that children are free from physical and psychological risks and that they are not exploited for commercial purposes.

5. Media organizations are encouraged to exercise self-regulation through responsibility in programming, publication or posting of any information affecting the physical, social, emotional, mental and moral development of the child. The publication of images or broadcast of programs containing information detrimental to child development should be shown or aired outside of the time slots allotted for children.

All journalists and media professionals have a duty to maintain the highest ethical and professional standards and should promote within the industry the widest possible dissemination of information about the International Convention on the Rights of the Child and its implications for the exercise of independent journalism.

Media organizations should regard violations of the rights of children and issues related to children's safety, privacy, security, their education, health and social welfare and all forms of exploitation as important questions for investigation and public debate.

Children have an absolute right to privacy, the only exceptions being those explicitly set out in these guidelines.

Journalistic activity which touches on the lives and welfare of children should always be carried out with appreciation of the vulnerable situation of children.

Journalists and media organizations shall strive to maintain the highest standards of ethical conduct in reporting children's affairs and, in particular, they shall:

Strive for standards of excellence in terms of accuracy and sensitivity when reporting on issues involving children;

Avoid programming and publication of images which intrude upon the media space for children with information which is damaging to them;

Avoid the use of stereotypes and sensational presentation to promote journalistic material involving children;

Consider carefully the consequences of publication of any material concerning children and shall minimize harm to children;

Guard against visually or otherwise identifying children unless it is demonstrably in the public interest;

Give children, when possible, the right of access to media to express their own opinions without inducement of any kind;

Ensure independent verification of information provided by children and take special care to ensure that verification takes place without putting child informants at risk;

Avoid the use of sexualized images of children;

Use fair, open and straight forward methods for obtaining pictures and whenever possible, obtain them with the knowledge and consent of children or a responsible adult, guardian or care giver;

Verify the credentials of any organization purporting to speak for or represent the interest of children;

Not make payment to children for material involving the welfare of children or to parents or guardians of children unless it is demonstrably in the interest of the child;

Journalists should put to critical examination the reports submitted and the claims made by Governments on implementation of the UN Convention on the Rights of the Child in their respective countries.

Media should not consider and report the conditions of children only as events but should continuously report the process likely to lead or leading to the occurrences of these events.



Simultaneous Symposium 1: **Online Child Abuse (Part I): Definitions, Laws and Reporting, Initial Investigation**

Manila Room, 2nd level Marco Polo Plaza
1:30 – 5:00 PM

AkoParaSaBata
APSB2015





Dr. Clara Nemia Antipala

*Providing Aftercare to Survivors
of Online Sexual Exploitation of Children (OSEC) in Cebu*

Case Study: Providing Aftercare to Survivors of OSEC in Cebu

Dr. Nemia Antipala
Director of Aftercare, IJM Cebu

Case Study: Major Impact of OSEC on Survivors

- Confused sense of right and wrong
- Attachment issues
- Trauma

Challenges in Providing Aftercare during Rescue

- Reducing trauma of rescue
- Providing developmentally appropriate information to survivors
- Protecting survivors' privacy

Challenges in Providing Aftercare Post-Rescue

- Lack of appropriate protective placements
 - Shelters
 - Foster Care
- Lack of expert care to manage trauma symptoms
- Permanency planning
- Engagement in legal case

Primary Needs of the Survivors

- Safe, trauma informed placement options immediate post-rescue
- Structure and return to normalcy
 - Return to a routine
 - Continuation of schooling
- Strong trauma services
- Long-term care options



with



and



present

AK PARA SA BATA THE INTERNATIONAL CONFERENCE IN CEBU

Theme:

CYBERPROTECTION OF CHILDREN

Cyber Safety of Children:
Internet and Mobile Protection for Minors



#AkParaSaBata
APSE2013

TEASER SS7: EFFECTIVE AFTERCARE FOR SURVIVORS OF ONLINE SEXUAL EXPLOITATION

OBJECTIVES: SS7

At the end of the session, the participants will be able to:

1. Describe promising practices from traditional trafficking and abuse and how they apply to survivors of online sexual exploitation;
2. Describe the short- and long-term emotional and psychosocial impact of online sexual exploitation; and
3. Describe trauma informed interventions in the aftercare of survivors of online sexual exploitation.

Program

1:30 – 1:45pm	INTRODUCTION
1:45 – 2:00pm	The Cebu Experience: Providing Aftercare to Survivors of OSEC <i>Dr. Nemia C. Antipala</i>
2:00 – 2:40pm	Applying Lessons Learned from Working with Survivors of Traditional Trafficking and Abuse <i>Ms. Ann Knapp, MSW</i>
2:40 – 2:50pm	OPEN FORUM
2:50 – 3:30pm	Emotional and Psychosocial Impact of Online Sexual Exploitation <i>Ms. Anamabel Garcia, MA</i>
3:30 – 3:45pm	BREAK
3:45 – 4:25pm	Importance of Trauma Informed Approaches <i>Dr. Jose Andres Sotto</i>
4:25 – 4:45pm	OPEN FORUM
4:45 – 5:00pm	Summary of Salient Points Evaluation

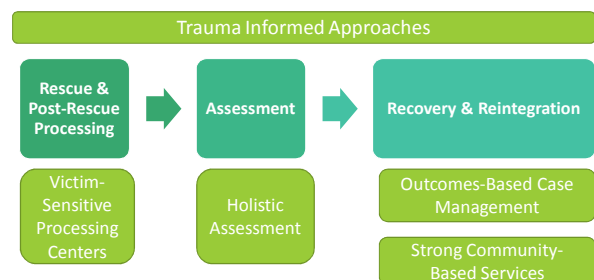
Applying Lessons Learned from Working with Survivors of Traditional Trafficking and Abuse: Key Points

1. Compare traditional trafficking and OSEC;
2. Review of best practices working with survivors of traditional trafficking; and
3. Discuss steps in preparing to apply lessons with survivors of online sexual exploitation of children.

Promising Aftercare Practices for Survivors of CSEC

1. Trauma informed approaches
2. Victim-friendly processing centers
3. Holistic assessment
4. Outcomes-based case management
5. Strong community-based services

Continuum of Aftercare



Preparing to Work with Survivors of OSEC

- Developing core competencies
 - Trauma Informed Care
 - Assessment
 - Forensic interviewing
 - Child development
 - Trauma-informed therapy
 - Family therapy
 - Case management
 - Managing challenging behaviors
- Resource mapping
- Forum for shared learning to adapt approaches

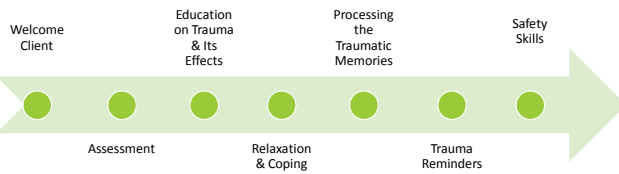
Emotional and Psychosocial Impact of Online Sexual Exploitation of Children: Key Ideas

- Forms of OSEC
- “Push” factors creating vulnerability to OSEC
- Unique challenges of providing care to survivors of OSEC
- Emotional and psychosocial impact of OSEC
- Hope of resiliency

The Importance of Trauma Informed Approaches: Key Points

- Foundations of trauma informed care
- Challenges in serving survivors of OSEC
- Domains of restoring attachment
- Examples of trauma informed approaches

Components of Trauma Informed Philippines Psychotherapy



AKO PARA SA BATA
THE INTERNATIONAL CONFERENCE IN CEBU

Child Protection Network with **ENERGEN** and **unicef** present

AKO PARA SA BATA

THE INTERNATIONAL CONFERENCE IN CEBU

Theme:

CYBERPROTECTION OF CHILDREN

Cyber Safety of Children:
Internet and Mobile Protection for Minors



#AkoParaSaBata
APSC2013