28 August 2015

ADVISORY ON ONLINE CHILD ABUSE

This Advisory is issued in the exercise of the Constitutional duty of
the State to protect the physical, moral, spiritual, intellectual and social
well-being of the youth, in light of reported incidents of online child
abuse. There is a need for stringent precautions by users, regardless of
age, and parents of minors who have unbridled access to computers and
the internet. In addition, this serves to remind internet service providers
(ISPs) of their obligations under the laws aimed to protect and secure the
rights of children online.

In this day and age, computers and internet have become essential
in offices, schools, establishments, and residences. Internet users
number about 2.92 billion. In the Philippines alone, roughly 37 million
out of its 98 million population are on the internet.¹

Younger age groups are more likely to go on the internet to upload
pictures and videos and network with each other. This can be associated
with the normal interest of youngsters during teenage years and which
usually include online gaming, watching videos, and establishing their
social circles. Studies reveal that there is a consistent increase in the
number of youth gaining access to the internet, thus, increasing the risk
of exposing them to online abuses.²

The internet has become a dangerous place for children and
teenagers with almost everything accessible at the click of a button. From
January to April 2015, the DOJ Office of Cybercrime (OOC), as the
Philippine Point-of-Contact for the National Center for Missing and
Exploited Children (NCMEC)³, received 8,035 reports from US
Electronic Service Providers (ESPs) and ISPs wherein either the offender
or the offended party is situated in the Philippines.

³NCMEC is a private non-profit organization granted a US Congressional authorization “to build a coordinated,
national response to the problem of missing and sexually exploited children, establish a missing children hotline
and serve as the national clearinghouse for information related to these issues.”
A great number of victims belong to the age group 13-17 years old, which might be due to the early exposure of children to technology. Better understanding of the complexities of the technologies exposes them to similarly complex interactions that involve greater risks. As NCMEC cites, about 93 percent of teens aged 12 to 17 years go online.

Another reason for increased risk is that the children are on the verge of puberty and sexual development. Online forums catering to these adolescents afford sexual offenders numerous opportunities to violate children’s rights. While most are keen on having romantic relationships, few are able to self-regulate and, thus, more likely to succumb to the deceit employed by supposed offenders. They tend to lack emotional control, act on impulse, and thereby disclose otherwise sensitive information that puts them at risk of sexual exploitation.

Child abuse is not new but the progress and greater access of information and communications technology (ICT) and its early introduction to children renders them more vulnerable, thereby aggravating the problem.

**APPLICABLE LAWS**

**A. UN Declaration on the Rights of the Child**

The Declaration of the Rights of the Child recognizes basic rights to which every child is entitled. It defines a child as “every human being below the age of eighteen years unless under the law applicable to the child, majority is attained earlier”. It states that a “child has the right to the protection of the law against such interference or attacks”. To this end, signatories must protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse. States are also expected to ensure that no child is subjected to any form of sexual abuse and exploitation. Corollary to this duty, every State must adopt measures to prevent “the inducement or coercion of a child to engage in any

---

6 UN General Assembly Resolution 1386(XIV) of 20 November 1959.
8 Article 16 (2), Ibid.
9 Article 19, Ibid.
unlawful sexual activity; the exploitative use of children in prostitution or other unlawful sexual practices; and the exploitative use of children in pornographic performances and materials.”

B. Lanzarote Convention

Emphasizing the obligation to protect the interests of children, the Council of Europe signed the Lanzarote Convention, recognizing that the “sexual exploitation and sexual abuse of children have grown to worrying proportions at both national and international level, in particular as regards the increased use by both children and perpetrators of information and communication technologies (ICTs).”

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

Pursuant to its commitment under the Convention on the Rights of the Child, the Philippines enacted Republic Act No. 7610 or the “Special Protection of Children Against Abuse, Exploitation and Discrimination Act,” (RA 7610) declaring the policy of the State “to provide special protection to children from all forms of abuse, neglect, cruelty exploitation and discrimination and other conditions, prejudicial their development.” This applies the policy of parens patriae, wherein the State shall formulate rules and programmes to prevent, prosecute, and punish any act tending to perpetrate such abuses. The State is also bound to provide counselling, rehabilitation and care for the victims.

As the general law for child abuse, RA 7610 defines child abuse as any maltreatment of a child including:

1. “Psychological and physical abuse, neglect, cruelty, sexual abuse and emotional maltreatment;

2. Any act by deeds or words which debases, degrades or demeans the intrinsic worth and dignity of a child as a human being;

Congress also defined specific forms of child abuse such as child prostitution and sexual abuse and trafficking.

---

10 Article 34, Ibid.
11 Section 2, Republic Act No. 7610 or the Special Protection of Children against Abuse, Exploitation and Discrimination Act.
12 Section 3, Ibid.
D. Republic Act No. 9775
Anti-Child Pornography Act of 2009

Congress enacted Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009," (RA 9775) which echoes the policy in RA 7610 and avows to -

"x xx

(b) Protect every child from all forms of exploitation and abuse including, but not limited to:

(1) the use of a child in pornographic performances and materials; and
(2) the inducement or coercion of a child to engage or be involved in pornography through whatever means xxx."15

In RA 9775, the State defines and penalizes a particular form of child abuse, which is child pornography. Under said law, child pornography is any representation of a child engaged or involved in real or simulated—

1. "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."16

Both RA 7610 and RA 9775 define a child as 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.17 RA 9775, however, includes a person regardless of age who is presented, depicted or portrayed as a child, as defined in the said law, 18 and any

13 Section 5, Ibid.  
14 Section 7, Ibid.  
15 Section 2, RA 9775.  
16 Section 3(c), RA 9775.  
17 Section 3 (a), RA 7610.  
18 Section 3(a) (1), RA 9775.
computer-generated, digitally or manually crafted image or graphics of a person who is represented or who is made to appear to be a child\textsuperscript{19}.

**E. Republic Act No. 9262**  
**Anti-Violence against Women and their Children Act of 2004**

Abuse in any form may happen at any time and under any circumstance. Abusers may be the parents, persons exercising parental or temporary authority over the child, adults who hold a position of trust in relation to a child, any stranger, or a child. Thus, a charge for violation of Republic Act No. 9262, or the “Anti-Violence Against Women and Their Children Act of 2004,” may be filed should the offender commit any act against a woman who is his wife, former wife, or against a woman with whom the person has or had a sexual or dating relationship, or with whom he has a common child, or against her child, which results or is likely to result in physical, sexual, psychological harm or suffering, or economic abuse.\textsuperscript{20}

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

Section 4 (c) (2) of the Cybercrime Law\textsuperscript{21} categorized the unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system, as a content related offense. Further, any child abuse related law, committed by, through and with the use of information and communications technologies, shall also be covered by the relevant provisions of the Cybercrime Prevention Act.\textsuperscript{22}

In *Disini vs. Secretary of Justice*\textsuperscript{23}, the Supreme Court upheld the validity of the above-mentioned provision, and stated that Section 4 (c) (2) of the Cybercrime Law “merely expands the scope of the Anti-Child Pornography Act of 2009 to cover identical activities in cyberspace. In theory, nothing prevents the government from invoking RA 9775 when prosecuting persons who commit child pornography using a computer system.” The law making the penalty more severe is a legislative prerogative and is justified by the fact that the potential for uncontrolled

\textsuperscript{19} Section 3(a) (2), RA 9775.  
\textsuperscript{20} Section 3, RA 9262.  
\textsuperscript{21} Republic Act No. 10175, or the “Cybercrime Prevention Act of 2012” (RA 10175).  
\textsuperscript{22} Section 6, Ibid.  
\textsuperscript{23} G.R. No. 205335, 11 February 2014.
proliferation of a particular piece of child pornography when uploaded in the cyberspace is incalculable.

ONLINE CHILD ABUSE

Child abuse may be categorized into six types – emotional abuse, neglect, physical abuse, family violence, sexual abuse, and organized sexual abuse. Sexual abuse may either be committed physically or online.

Online child abuse is defined as the “searching for, sharing and downloading of images of children being physically and sexually abused and approaching children online with the intention of developing a sexual relationship in the ‘real’ world (so-called "grooming").” Approaches may involve the assumption of a false identity, in particular the pretense of being a child, although this is not always the case. Other forms of online child abuse include sending indecent or obscene images to a child, soliciting from them indecent images of themselves or their friends, engaging them in sexually explicit talk and encouraging them to perform sexually explicit acts on themselves or their friends.

The prevalent abuses are sexual in nature, such as grooming and sexting. However, non-sexual abuses can also be committed online, as in the case of cyberbullying.

Grooming are actions by an adult who establishes emotional connection with a child designed to lower a child’s inhibitions in preparation for sexual activity or exploitation.

Sexting is the act of “sending of sexually explicit messages or images by cell phone.” This is different from the normal sending of text messages or ‘texting’. In sexting, sexual messages or nude/semi-nude images are transmitted.

On the other hand, cyberbullying is the act of threatening or intimidating someone committed by, through and with the use of technology such as text messaging, website postings, and the like. This is similar to bullying in a physical face-to-face environment but what sets it

---

apart is the medium used and extent to which the intimidation is made public.

Child sexual abuse images may be classified into five (5) categories, based on the 10-point typology developed by COPINE—a rating system created in Ireland and used in the United Kingdom to rank the severity of images of child sex abuse, to wit:

a. Images depicting nudity or erotic posing with no sexual activity;
b. Sexual activity between children, solo masturbation;
c. On-penetrative sexual activity between an adult and a child;
d. Penetrative sexual activity between an adult and a child; and

e. Sadism or bestiality.”

Profiling offenders

The conception that adults are the only perpetrators no longer applies today as even kids and teens commit abuse against their same age groups. This may be attributable to early exposure to a myriad of technology and information. In several instances, those who used to be victims became offenders themselves. Hence, there can be no one type of child sex offender even if there were consistent patterns of gender and age among offenders. It would be wrong to assume that offending fits a homogenous profile. Types of offenders include:

1. **Browser** - indirect offenders who stumble upon child abuse images but knowingly saves them. While browsing may not be an offense, intentionally storing or keeping them in file is an offense;

2. **Private fantasizer** – conscious creators of online child exploitation materials for his personal use. Thinking of having sex with a child is, while morally wrong, not an offense but expressing it in a manner that can be preserved is;

---


27 Ibid, page 5.

3. **Trawler** – the sexually curious who actively seeks child abuse materials through openly available browsers. This may already involve networking;

4. **Non-secure collector** – they openly seek materials through chat rooms and peer-to-peer networks which are not secure;

5. **Secure collector** – active seekers who have the need to collect and willing to exchange materials but over secure connections. Usually, they are involved in secret pedophile rings and high-level networking observing sophisticated security measures. Some have entry requirements for the purpose of protecting everyone in the group and each is required to submit photos or videos;

6. **Groomer** – those who intentionally establish online relationships with a child by sending pornographic materials to the child;

7. **Physical abuser** – direct sexual abusers who document their exploits which they may or may not share;

8. **Producer** – offenders who record abuses by others for purposes of dissemination; and

9. **Distributor** – may have purely financial interest or any of the above offender who distributes child abuse images.

It has to be noted that in no instance was an offender described as a male. In a statistical report by the US DOJ in year 2000, even females engaged in child sexual exploitation. Thus, the foregoing classification applies to both genders.

**Vulnerable age group**

The NCMEC noted a dramatic increase in cases of exploitation of children since the 1990s based on a report by US Congress in 2010. Between the years 2004 and 2008, there was a 230 percent increase in the number of documented complaints of online enticement of children. NCMEC’s CyberTipline already received more than 3.3 million reports of suspected child sexual exploitation since in 1998.²⁹

A great number of the victims belong to the age group 13-17 years old, which might be due to the early exposure of children to technology.

Better understanding of the complexities of the technologies exposes them to similarly complex interactions that involve greater risks. As NCMEC cites, about 93 percent of teens aged 12 to 17 years go online.

Another reason for increased risk is that children are on the verge of puberty and sexual development. Online forums catering to these adolescents afford sexual offenders numerous opportunities to violate children’s rights. While most are keen on having romantic relationships, few are able to self-regulate and, thus, more likely to succumb to the deceit employed by supposed offenders. They tend to lack emotional control, act on impulse, and thereby disclose otherwise sensitive information that puts them at risk of sexual exploitation.

Impact on a child

Childhood abuse has been found to cause depression, anxiety disorders, addictions, personality disorders. Abuses also cause eating disorders, sexual disorders and suicidal behavior. A study with 384 survivors of childhood abuse found that they tend to be depressed, have low self-esteem, and have problems with family functioning. Almost 76% of adults reporting child physical abuse and neglect have at least one psychiatric disorder in their lifetime and nearly 50% have three or more psychiatric disorders. Furthermore, child sexual abuse has been found to be a key factor in youth homelessness. The impacts of child abuse can last into adulthood and interfere with a person’s general outlook in life.

ADVISORY

1. Internet Service Providers (ISPs) must block or filter child pornography websites.

The law mandates that ISPs must block child pornography websites by installing available technology, program or software.

---

32 Draper et al., (2007)
33 Palmer, Brown, Rae-Grant, & Loughin, (2001)
34 Harper et al., (2007)
35 van Loon & Kraik, (2005)
Section 9 of RA 9775 provides:

“Section 9. Duties of an Internet Service Provider (ISP).— 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. Nothing in this section may be construed to require an ISP to engage in the monitoring of any user, subscriber or customer, or the content of any communication of any such person: Provided, That no ISP shall be held civilly liable for damages on account of any notice given in good faith in compliance with this section.

Furthermore, an ISP shall preserve such evidence for purpose of investigation and prosecution by relevant authorities.

xxx

All ISPs shall install available technology, program or software to ensure that access to or transmittal of any form of child pornography will be blocked or filtered.”

Consequently, the law penalizes ISPs who violate said mandate. For the first offense, Section 15 (k) of R.A. 9775 provides a fine ranging from Php 500,000.00 to Php1,000,000.00 and from Php1,000,000.00 to Php2,000,000.00 with revocation of license to operate for subsequent offenses.

Section 10, par.2, of the same law requires photo developers, information technology professionals, credit card companies and banks and any person who has direct knowledge of any form of child pornography activities to report any suspected child pornography materials or transactions to the proper authorities. It creates a conclusive presumption of knowledge of commission of child pornography against mall owners/operators and owners or lessors of other business establishments when there is a public display of any form of child pornography within their premises.

In connection with this, the National Telecommunications Commission (NTC) issued a circular in accordance with the legal requirement. Memorandum Circular No. 01-01-2014 requires ISPs to furnish “at least three (3) carrier grade technology, program or software solutions to the IACACP for evaluation.” NTC, on the other hand, will furnish the ISPs a list of pornographic websites provided by

---

36 NTC M.C. No. 01-01-2014, (2).
the Inter-Agency Council Against Child Pornography (IACACP) for blocking. Within five (5) days from the end of each month, ISPs will report to IACACP the websites that they have blocked.

The DSWD-ICTMS suggested that the blocking/filtering technologies shall have specific proactive and dynamic blocking technologies that address child pornography. This is consistent with the duty of ISPs to notify the Philippine National Police (PNP) or the National Bureau of Investigation (NBI) within seven (7) days from obtaining facts and circumstances that any form of child pornography is being committed using its services or facility. ISPs may comply with their duty to report the commission of child pornography by using hash value calculation or photoDNA (pDNA) technology.

The DOJ-OOC issued a legal opinion providing that the DSWD-ICTMS minimum specifications of the blocking/filtering technology are consistent with NTC MC 01-01-2014. Further, ISPs do not violate the rights on privacy of communications and correspondence, or the laws on data privacy, as the activity to block/filter child pornography is justified by a compelling state interest—to protect the child from all forms of exploitation and abuse.

2. ISPs shall, upon request of proper authorities, furnish the particulars of users who violated the child pornography law.

ISPs shall report the commission of child pornography in their servers or facilities to law enforcement authorities. Upon request of proper authorities, ISPs are mandated to furnish them the particulars of users who gained or attempted to gain access to an internet address which contains any form of child pornography, without need of a court warrant.

Section 9 of RA 9775 provides:

"Section 9. Duties of an Internet Service Provider (ISP). – x x x

An ISP shall, upon the request of proper authorities, furnish the particulars of users who gained or attempted to gain access to an internet address which contains any form of child pornography. x x x"
Service providers are required to cooperate and assist law enforcement authorities in the collection or recording of the above-stated information.

3. **Parents must instruct children to be SMART.**

Parents must teach their children to be SMART when going online:

- **S – SAFE.** Keep safe by being careful not to give out personal information – such as your name, email, phone number, home address, or school name – to people who you do not know online.

- **M – MEETING.** Meeting someone you have only been in touch with online can be dangerous. Only do so with your parents'/carers' permission and when they can be present.

- **A – ACCEPTING.** Accepting e-mails, IM messages or opening files from people you do not know or trust can be dangerous – they may contain viruses or nasty messages.

- **R – RELIABLE.** Someone online may be lying about who they are, and information you find on the internet may not be reliable.

- **T – TELL.** Your parent, guardian, or a trusted adult if someone or something makes you feel uncomfortable or worried.\(^{37}\)

Get your child to understand that the absence of physical contact does not remove it from the definition of abuse. Adults, themselves, must be able to understand that our realities are no longer limited to the physical. There must be a realization that non-physical acts can damage just as much as the physical.

4. **Parents should pay attention to your kids’ online activities.**

Track the pages and sites visited by your child as well as the materials he/she downloads and uploads. Check on the information that your child may have uploaded that may be manipulated by offenders who would come across it. You may do this without actually watching over his shoulder. Computers keep cookies, caches, and history of pages visited. Some internet service providers offer software or services with parental control or child safety features. Placing computers in places

---

37 Parents Protect, Childnet SMART rules, Accessible at: www.parentsprotect.co.uk.
where everyone can see what is being viewed can also be a deterrent from potential abuse. Monitoring time spent online will ensure it does not become excessive.

Also, know who their friends are, both offline and online. Get to know who they have been communicating with often and with what frequency. Find out conversation topics and circumstances surrounding the formation of those relationships.

For the less computer-savvy adults, you may seek help in understanding for yourself advanced information about computers that will help you protect your child. Netsmartz 411 is an online resource for adults’ questions concerning Internet safety, computers and the Web.

5. Keep communication lines open.

It cannot be over emphasized that communication is a key. Parents should avoid police interrogation-like questioning. Instead, phrase question with non-threatening words. By eliminating fear between you and your child will allow exchange of information needed to further your purpose. Have constant communication where you can alternately ask questions and explain concepts whenever needed.

Keep in mind that sexual offenders were able to gain the confidence of children because they were able to empathize with them. Likewise, try to gain the child’s confidence instead of alienating his feelings and prevent him from disclosing possible risks to his safety. Ask what his interests are and learn to share his enthusiasm for the same. Explain how their interactions, activities, and disclosures online could affect them, particularly the dangers that the internet present.

Learn the acronyms used in the chatrooms frequented by your child. There are sites which list as many acronyms as the administrators can gather from other sites where they are used or coined.

6. The public should report child exploitation images.

Reports of any forms of online child abuse may be made to any of the following offices:

- Department of Justice-Office of Cybercrime
  Tel No. 523-0628
  cybercrime@doj.gov.ph
• National Bureau of Investigation-Cybercrime Division
  Tel No. 532-8231 to 38 local 3454 and 3455
  ccd@nbi.gov.ph

• National Bureau of Investigation-Anti-Violence Against Women
  and Children Division
  Tel No. 525-6028/302-7623
  vawcd@nbi.gov.ph

• Philippine National Police-Anti-Cybercrime Group Angelnet
  Tel No. 4141560
  pnp.acg.angelnet@gmail.com

• Inter-Agency Council Against Child Pornography (IACACP)
  iacacp.gov.ph/report-to-us-2

  IACACP also receives reports of child pornographic sites through
  SMS. Key in DSWD<space>blockchildporn<space>URL address then
  send to 2327. Or send blockchildporn<space>URL address to
  09189122813.

  This Advisory is issued in light of the emerging trend in law
  enforcement and in line with the priority of the Department of Justice
  Office of Cybercrime to prevent commissions of online child abuse. All
  are hereby enjoined to disseminate and faithfully observe this advisory.

  LEILA M. DE LIMA
  Secretary
  Department of Justice
  CN: 020150007