Republika ng Pilipinas
KAGAWARAN NG KATARUNGAN
Department of Justice
Manila

DEPARTMENT OF JUSTICE
OFFICE OF CYBERCRIME
ADVISORY OPINION NO. 001 (SERIES OF 2023)
30 June 2023

ADVISORY ON THE NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN AND ITS CYBERTIPLINE REPORT

This Advisory is being issued by the Department of Justice (DOJ) – Office of Cybercrime (OOC) for the information and guidance of the criminal justice sector players, especially the law enforcement agencies (LEA) and prosecutors, regarding investigative leads or reports from the National Center for Missing and Exploited Children (NCMEC) (CyberTipLine Report [CTR]).

INTRODUCTION

NCMEC is a private non-profit organization incorporated in the United States in 1984 by child advocates to serve as a national clearinghouse and resource center for families, victims, private organizations, LEA, and the public on missing and sexually exploited child issues. To fulfill its mission, it operates the "CyberTipline"—a centralized reporting system for online exploitation of children. It receives reports about suspected incidents of sexual exploitation of children online and makes information available to LEA and likewise works with Electronic Service Providers (ESP) to reduce online child sexual abuse images.

As a private organization, NCMEC does not act in the capacity of, or under the direction or control of, the government or LEA. NCMEC also does not investigate and cannot verify the accuracy of the information submitted by reporting parties.

In the Philippines, the DOJ-OOC is designated as the central authority in all matters related to international mutual assistance and extradition for cybercrime and cyber-related matters.[1]

CYBERTIPLINE REPORT

The United States' Protect Our Children Act of 2008 provides that ESPs must make a report to NCMEC of any known facts or circumstances from which there is an apparent criminal offense involving child sexual abuse or exploitation materials (CSAEM).[2] NCMEC, in turn, is mandated by such statute to make each CTR

---

[1] Section 23, Republic Act No. 10175.
[2] 18 U.S.C. Section 2258A(a)(1)-(2).

available to federal law enforcement.[3] Most of the time, the ESPs block, remove, or take down accounts within their systems that are reported to NCMEC.

The CTR contains information identifying the user and other information relating to the reported person, victim, and the apparent CSAEM. This information may have been reported by individuals or the ESPs themselves. Once received in the CyberTipline, NCMEC analyzes the data. Automated information added by the NCMEC system includes a potential location for the incident to make it available to the appropriate LEA for possible investigation.

Should the reported information appear to involve a foreign country in which there is a designated LEA that has established a secure connection to NCMEC's CyberTipline, such as the Philippines, this report will be automatically referred to the designated international LEA for potential evaluation, investigation, and/or prosecution.

Thus, investigations into violations of Republic Act (R.A.) No. 11930, otherwise known as the "Anti-Online Sexual Abuse or Exploitation of Children (OSAEC) and Anti-Child Sexual Abuse or Exploitation Materials (CSAEM) Act" and/or R.A. No. 11862 or the "Expanded Anti-Trafficking in Persons Act of 2022," may begin with the receipt of a CTR from NCMEC.

In 2022, the DOJ-OOC received a total of 2,539,864 CTRs.[4]

LEGAL FRAMEWORK

A. Budapest Convention on Cybercrime

The Budapest Convention on Cybercrime (BCC) is the first international treaty aimed at addressing computer-related crimes by harmonizing national laws, improving investigative techniques, and enhancing international cooperation among nations. In order to provide cooperation to the widest extent possible, Article 35 of the BCC mandated the establishment of the 24/7 Network as a tool for expedited international cooperation on cybercrime and electronic evidence.

The Philippines acceded to the BCC and became an official member thereof in July 2018. The designation of the DOJ-OOC as the 24/7 Network in the Philippines in line with Article 35 of the BCC is embodied in the Note Verbale dated 28 March 2018 issued by the Embassy of the Republic of the Philippines in Paris. The Note Verbale and the accession package to formalize the Philippines' membership to the BCC were deposited with the Secretary General of the Council of Europe (COE).

---

[3] Id. Section 2258A(c)

[4] It is worth noting that the statistics mentioned above mostly include multiple generated CTRs on the same content (*as when content becomes viral and sent multiple times to different users*), misleading digital images (*such as nude photos of children generated by their parents in good faith*), and inaccurate reporting by electronic communication service providers (*human intervention leading to mistakes in reporting*).

B. R.A. No. 10175, otherwise known as the "Cybercrime Prevention Act of 2012"

Prior to its membership, the BCC already provided the Philippines with a legal framework that resulted in the legislation of the country's first comprehensive law on cybercrime—R.A. No. 10175, otherwise known as the "Cybercrime Prevention Act of 2012." As a form of compliance with the 24/7 Network requirement of the BCC, the DOJ-OOC was created under R.A. No. 10175 to cope with the complex, technical, and trans-border nature of cybercrimes and cyber-related offenses, as well as to meet the BCC's objective of achieving a fast and effective regime of international cooperation among nations.

Notably, the BCC's Explanatory Reports and Guidance Notes provide an in-depth explanation on the concept of establishing both the Central Authorities and 24/7 Network i.e., to promote, to the widest extent possible, cooperation between and among members. These cooperative arrangements may cover investigations of cybercrimes and the gathering of electronic evidence. Cooperation is likewise encouraged in the area of information sharing, specifically in the real time collection of traffic data and interception of content data.

"International mutual assistance" in Section 23 of R.A. No. 10175, therefore, does not only pertain to mutual legal assistance, but also to requests for assistance to conduct investigations and the gathering of electronic evidence.

Pursuant to the foregoing, the DOJ-OOC was designated the point of contact in the Philippines for the CyberTipline pursuant to a policy agreement executed in 2014 between the DOJ and NCMEC. This makes available to the DOJ-OOC the reports NCMEC receives that have a Philippine nexus through the NCMEC portal. The DOJ-OOC receives and conducts initial investigation on these reports. If the same is found to be actionable, the DOJ-OOC refers these CTRs to the relevant agencies and offices—primarily operational law enforcement units—for appropriate action.

C. R.A. No. 11930, otherwise known as the "Anti-Online Sexual Abuse or Exploitation of Children and Anti-Child Sexual Abuse (OSAEC) or Exploitation Materials Act (CSAEM)"

R.A. No. 11930 expressly repealed R.A. No. 9775 or the Anti-Child Pornography Act of 2009. The latest law describing and penalizing OSAEC and CSAEM strengthed the government's fight against the same by imposing stricter duties and responsibilities to the internet intermediaries.[5] These duties and responsibilities include, but are not limited to, reporting to the DOJ, within three (3) days, the internet address or websites blocked, removed or taken down, or any form of unusual data activity using its server or facility.

[5] Section 9, Republic Act No. 11930.

In cases when a foreign internet intermediary is prohibited by its country to share data, the reports filed by such foreign internet intermediary to the corresponding entity tasked by its government to receive cybercrime reports shall be deemed in compliance with its reporting duty under R.A. No. 11930.

The foregoing notwithstanding, the said foreign internet intermediary shall inform the DOJ of such reporting: Provided, further, That whatever relevant evidence otherwise not prohibited by law to be shared shall nevertheless be reported to the DOJ.

D. R.A. No. 11862, otherwise known as the "Expanded Trafficking in Persons Act of 2022"

R.A. No. 11862 is a further enhancement of the existing anti-trafficking in persons laws in the Philippines. It included as a purpose for trafficking in persons the act of engagement of others for the production or distribution, or both, of materials that depict child sexual abuse or exploitation materials, or other forms of sexual exploitation.[6]

Consequently, R.A. No. 11862 likewise imposes stricter duties and responsibilities to internet intermediaries including, but not limited to, the reporting and blocking, removal, or take down duties, as described in the immediately preceding section of this Advisory.

ADVISORY

In view of the foregoing, the following points are stated:

A. PROCESS OF HANDLING CTRs

To understand the nature of CTRs, the following illustrates the process how the CTR is referred to the appropriate agency by the DOJ-OOC:

1. NCMEC receives reports from the public or ESPs.
2. NCMEC applies human and/or computer analysis to identify indicators of risk and add value to the reports. For those with a Philippine nexus, NCMEC makes the reports available to the DOJ-OOC.
3. DOJ-OOC receives the CTRs designated for the Philippines and reviews and evaluates them to identify the appropriate action, including deciding the proper office or agency to refer reports for further investigation, intervention, and/or enforcement, as may be appropriate.
4. Philippine government agencies—primarily operational law enforcement units—receive the CTRs from DOJ-OOC and take the necessary action thereon.

[6] Section 3 (a), Republic Act No. 11862.

Based on the foregoing, the CTR, when received by the operational law enforcement units, are treated as investigative leads, tips, or reports to initiate further investigation.

It is important that LEA pay attention to CTRs and follow up on leads in a timely manner as ESPs may have relatively short retention periods for this data.

B. CONTENTS OF THE CTR

The CTR is divided into different sections: the reported information, automated information added by NCMEC systems, additional information provided by NCMEC, and the contact information of LEA.

The CTR contains identifying information on the person or ESP who reported the incident, the reported persons, and the child victims, details for the date and time of the incident, web and IP addresses, internet service provider that owns or controls the IP address, approximate geolocation data, hash values, file names, and other helpful contextual facts.

CSAEM are not shown or included in the body of the CTR but may be accessed by authorized LEA using the NCMEC Case Management Tool.

C. CTRs ARE TREATED AS INVESTIGATIVE LEADS OR REPORTS TO INITIATE INVESTIGATIONS

While relying solely on the information provided in CTRs may not be sufficient to apply for the necessary warrants, nor does the information therein constitute facts personally known to LEA, LEA and prosecutors may still use the information received as the basis for investigation and as leads or tips to conduct separate case build-up. The CTRs contain information to locate and identify subjects and especially child victims, so the appropriate protection and intervention actions may be carried out.

In most cases, additional information will need to be acquired to get subscriber, traffic, and content data, and other context needed to ultimately support charges for violations of Philippine laws.

There are eight (8) categories of reporting in the CyberTipLine: (1) Child pornography (possession, manufacture, and distribution); (2) Online enticement of children for sexual acts; (3) Child sex trafficking; (4) Child sexual molestation; (5) Child sex tourism; (6) Misleading domain name; (7) Misleading words or digital images on the internet; and (8) Unsolicited obscene material sent to a child. NCMEC definitions are based on United States law. However, NCMEC does not view its designations of offenses to be definitive and does not consider itself as the determiner of what is legal or illegal. It relies on LEA to do their own independent investigation, evaluation, and assessment of a file and/or reports.

D. DUTY OF INTERNET INTERMEDIARIES TO REPORT OSAEC AND CSAEM CASES

Both R.A. Nos. 11930 and 11862 require internet intermediaries to adopt in their terms of service or service agreements with third-party users or creators of contents, products, and services the prohibition of any form or any conduct of streaming or livestreaming of OSAEC and CSAEM in the use of their website, platform, server or facility.

Furthermore, both laws require internet intermediaries to report to the DOJ the internet address or websites blocked, removed, or taken down, or any form of unusual activity using its server or facility. Generally, ESPs immediately act on OSAEC and CSAEM reports by blocking, removing, or taking down accounts and site URLs prior to submitting reports to NCMEC.

Accordingly, for foreign internet intermediaries mandated to report to NCMEC, which CTRs are ultimately reported to the DOJ-OOC, reporting to NCMEC shall be deemed compliance with their reporting duty under R.A. Nos. 11930 and 11862.

This Advisory is issued by the DOJ-OOC in line with its mandate to issue and promulgate guidelines, advisories, and procedures in all matters related to cybercrime and cyber-related investigation, and as the focal agency in formulating and implementing law enforcement investigation and prosecution strategies in curbing cybercrime and cyber-related offenses. All are hereby enjoined to disseminate and faithfully observe this Advisory.

JESUS CRISPIN C. REMULLA
Secretary

Department of Justice
CN: O202402147