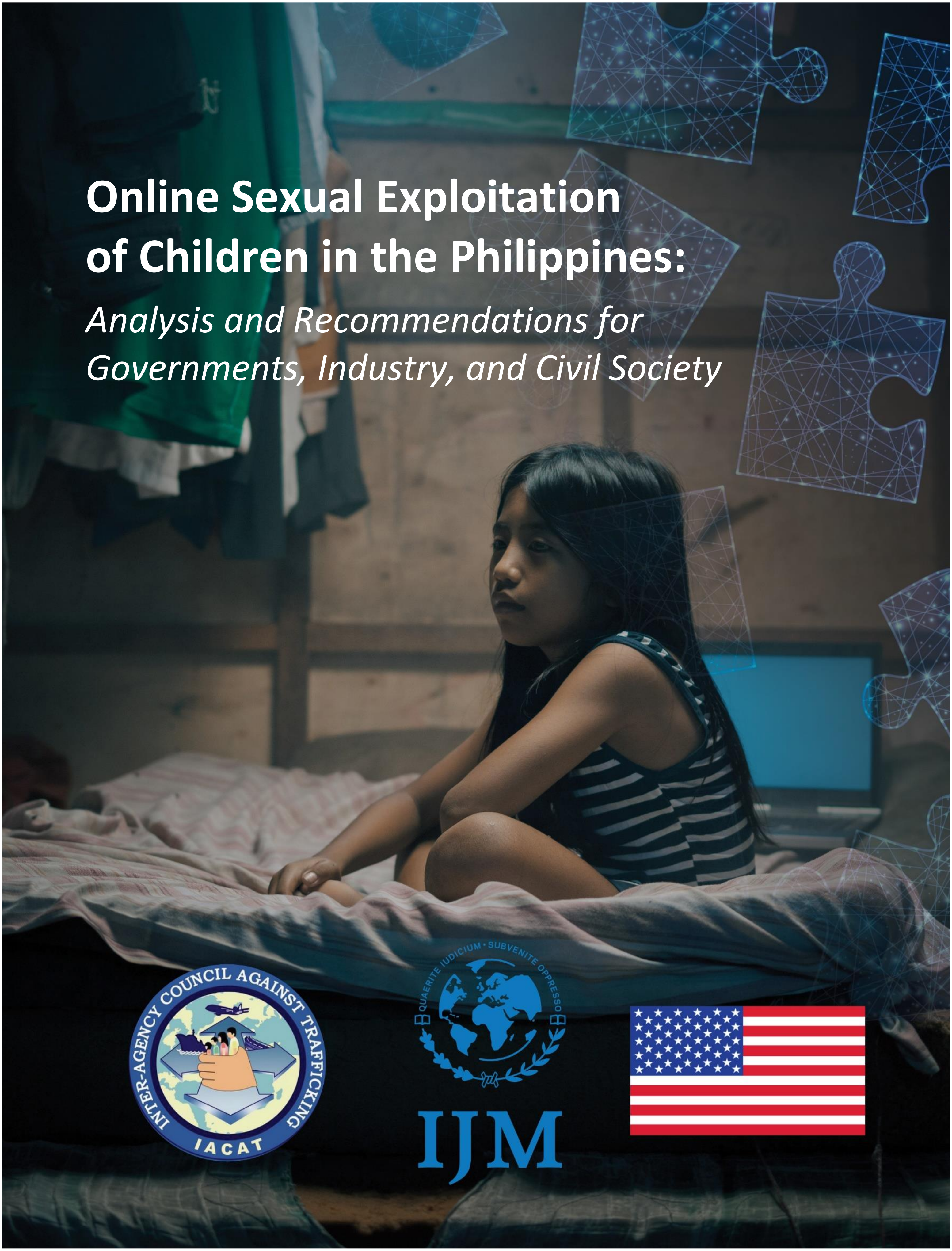
Online Sexual Exploitation of Children in the Philippines:

Analysis and Recommendations for Governments, Industry, and Civil Society



INTER-AGENCY COUNCIL AGAINST TRAFFICKING
IACAT

QUAERITE IUDICIUM • SUBVENITE OPPRESSO
IJM

Foreword

The sexual exploitation of children is, sadly, not a new phenomenon. It has existed for many centuries, has victimized children of any age from all countries, and has been committed by offenders of all backgrounds from around the world. What has changed however, are the ways in which these offences occur and the mechanisms that facilitate these types of abuse.

In the last fifteen years there has been a significant increase in the use of technologies internationally. Across much of the globe, it is hard to find a person without at least one mechanism that allows them to access the Internet at the mere touch of a button. However, as history will teach us, with every new invention there will be misuse - this has never been more evident than with online technologies and the Internet.

Technological advancements have changed the ways through which children are sexually exploited – online child sexual exploitation continues to grow exponentially with hotlines around the world reporting a consistent and continual increase in number of cases every year. Efforts internationally are responding to these increases. We are seeing police agencies utilizing technology to help them further investigations and more and more industry partners are exploring how they can be part of the solution. Additionally, non-government agencies continue to seek out new opportunities to enhance their support to victims in their communities through supporting criminal justice and social service system development, survivor care, and community-based support mechanisms. Never before has it been more important to work together to protect children. But in order to do just that, it is imperative that we know more about these crimes against children. We must know how they are occurring, who is committing them, and who is being victimized in order to more fully protect this vulnerable population.

Sexual exploitation, on- and off-line, has always been and continues to be a difficult area to measure – those of us in this area of study are repeatedly asked questions such as “is there more sexual exploitation now than before,” “how many children are exploited per year” and so on. These questions are almost impossible to answer, particularly when using only one source of data – data that has been obtained through formal channels of reporting. This comes with a significant limitation: sexual exploitation of children, on- and off-line is often underreported. There are several reasons why children do not report abuse. For example, some do not know that what they are experiencing is abuse; some are being abused by those who should protect them etc. among many other reasons. There is no one statistic that can tell us the prevalence nor the modus operandi of these crimes. Further complicating this is the reality that there are often jurisdictional differences – we define these types of abuse differently, generally contextualized by where we live in the world and our legislative framework. What does stay consistent and keeps up aligned is our common commitment and adherence to the United Nations (UN) Convention on the Rights of the Child which seeks to uphold every child’s right to be free from various forms of harm, including sexual exploitation, regardless of where they live. These standards are the threads that link us together in our obligation to protect children.

We then find ourselves in a situation where we must gather different types of data to try to piece together the reality of these crimes in order to advance our understanding and to inform our response strategies. It is symbolic of a jigsaw puzzle – many of us hold different and important parts of the answer but we must work together to develop a more holistic picture of these crimes – we must fit all of the pieces together. Similar to the frustration some of us might have experienced as a child when a sibling stole the last piece of our puzzle, when we experience barriers to sharing information we may feel frustrated as our puzzle is not complete – our understanding of the online sexual exploitation of children is not complete unless we all work together and share what we know when possible.

This is what this report represents – a starting point to trying to answer important and complex questions concerning the online sexual exploitation of children – a start to putting together that complex puzzle by thinking about how we can use the data we have to help to protect children. This initial picture then gives all stakeholders some suggestions for improving how we identify, track and respond to these emerging crimes, which then will allow us to continue to piece the puzzle together. This is similar to the approach of the Virtual Global Taskforce - an international alliance of police, Industry and non-government agencies working together to better protect children from online child sexual exploitation and other forms of transnational child sexual exploitation. The VGT recognizes the importance of all of our work in bettering the world for children. The contributions that International Justice Mission make in this area are noteworthy and encourage us all to continue to seek out ways in which we can continue to work together – to make this puzzle more complete. Children globally deserve nothing less.

Dr. Roberta Sinclair

Virtual Global Taskforce Secretariat Member

Table of Contents

List of Tables

List of Figures

Definitions and Key Terms

The purpose of this section is to provide definitions and explanations of key terms associated with OSEC to provide a common understanding of terminology as well as the individuals, platforms, and groups involved in the crime.

ONLINE SEXUAL EXPLOITATION OF CHILDREN (OSEC)

The production, for the purpose of online publication or transmission, of visual depictions (e.g., photos, videos, live streaming) of the sexual abuse or exploitation of a minor for a third party who is not in the physical presence of the victim, in exchange for compensation.

> Clarifying note: International Justice Mission's program targets a specific subset of online exploitation of children as laid out above. This definition is a functional definition for IJM and its partners to guide efforts to address this specific issue in accordance with local Philippine law. The global community uses a number of terms related to this crime, including both broader, umbrella terms under which IJM's definition of OSEC falls (such as trafficking, child sexual abuse, or internet crimes against children), and more specific terms that may apply in OSEC cases (such as livestreaming, child sexual abuse to order, etc.). Further information on OSEC and why this research study focuses specifically on this issue as defined above is provided in the introduction and literature review sections. Where possible, IJM aligns its terminology with the Luxembourg Guideline; readers are encouraged to reference these Guidelines for a more in-depth exploration of terms and associated issues.[1]

CHILD/MINOR

A person below eighteen (18) years of age but also any person over eighteen (18) years of age who is unable to fully protect himself/herself from abuse, neglect, cruelty, exploitation or discrimination, or who is unable to care for himself/herself because of a physical or mental disability or condition. [2]

CHILD PORNOGRAPHY

Any representation, whether visual, audio, or written combination thereof, by electronic, mechanical, digital, optical, magnetic or any other means, of a child engaged or involved in real or simulated explicit sexual activities.[3] Note: This term is sensitive, and use should be limited to legal contexts, as necessary, such as referring to statutes against child pornography. IJM more commonly uses the term CSEM as defined below.

CHILD SEXUAL EXPLOITATION MATERIAL (CSEM)

Any visual or audio (and/or any combination thereof) representation of minors under the age of 18 engaged in sexual activity or of minors engaging in lewd or erotic behavior recorded, produced and/or published to arouse the viewer's sexual interest. Child sexual abuse material (CSAM), which depicts the contact sexual abuse of a child, is a subset of CSEM. This report will use CSEM as a broad, umbrella term.

[1] ECPAT Luxembourg/ECPAT International (2016). "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse". Retrieved from http://cf.cdn.unwto.org/sites/all/files/docpdf/terminologyguidelines.pdf

[2] This definition is consistent with Philippine law, See e.g., http://www.lawphil.net/statutes/repacts/ra2009/ra_9775_2009.html

[3] See Anti Child Pornography Law (RA 9775). Consistent with the Luxembourg Guidelines for appropriate terminology, IJM refers to Child Pornography as Child Sexual Exploitation Material (CSEM) except when referring to legal statutes and definitions that use the term Child Pornography.

CYBERTIPLINE REPORT

Reports received by the National Center for Missing & Exploited Children (NCMEC) from the public and ESPs related to child sexual exploitation. NCMEC makes CyberTipline reports available to law enforcement agencies around the world as appropriate, based on apparent jurisdiction related to the reported incident.

DARK WEB

The part of the World Wide Web that is only accessible by means of special software, allowing users and website operators to remain anonymous or untraceable.

ELECTRONIC SERVICE PROVIDER

Electronic service providers (ESPs) provide communication services via the internet or other electronic platforms.

INTERNET CRIMES AGAINST CHILDREN (ICAC)

A term primarily used by law enforcement to denote internet-facilitated crimes against children. Many law enforcement agencies have ICAC investigators or task forces assigned to investigate and respond to online crimes such as OSEC, sextortion, possession or distribution of CSEM, etc.

LIVESTREAMING OF CHILD SEXUAL ABUSE

Child sexual abuse that is transmitted to a viewer/s in real time through "streaming"[4] over the internet. Abuse video is transmitted instantaneously to the viewer, who can watch, engage, and even direct abuse while it is occurring. This can take both commercial and non-commercial forms.[5]

MONEY TRANSFER AGENCY

Agencies and platforms that provide international money transfer and payment services between individuals and/or institutions. OSEC traffickers in the Philippines typically receive payment from OSEC customers via money transfer agencies.

OSEC CUSTOMER[6]

Any person who provides financial compensation to an OSEC trafficker or child for any form of CSEM or for any in-person sexual exploitation of a minor. Customers in OSEC cases typically actively participate in the sexual abuse of the minor/s through requesting or dictating abuse to order in advance and/or directing abuse as it occurs via livestream (see livestreaming definition above). OSEC customers also produce CSEM when they record sexual abuse remotely and when they entice, solicit, or coerce minors to create CSEM. Although they are offenders, they are referred to in this report as "customers" to easily distinguish them from traffickers and highlight the commercial nature of their crime.

[4] Streaming is a technology that consists of playing data before the entire file has been transmitted, sending the information directly to the computer or device of the recipient (via a webcam, audio interface, etc.) without any need to save the file onto a hard disk (although streaming material can also be recorded and saved to a file). Unless the content is deliberately recorded, it is available only on one occasion and leaves no trace on the device once it has been viewed. In relation to online child sexual exploitation cases, most of the incidents that relate to live streaming involve real-time production and transmission of the audio/video data through the webcam at the victim's end. (Luxembourg Guidelines)

[5] ECPAT Luxembourg/ECPAT International (2016). "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse". Retrieved from http://cf.cdn.unwto.org/sites/all/files/docpdf/terminologyguidelines.pdf

[6] Note: both the sale (facilitation by the domestic "trafficker") and the purchase (offending by the foreign "customer") of OSEC are criminal acts that violate the human trafficking laws in the Philippines and the UN Protocol to Prevent, Suppress and Punish Trafficking in Persons (Palermo Protocol). For the sake of clarity and readability in this report, the terms OSEC Customer and OSEC Trafficker are used to differentiate between the roles of the criminals involved in this trafficking offense.

OSEC TRAFFICKER

Any person who sexually abuses or exploits a child through the means of the internet through offering CSEM and/or a minor or adult[7] for the purpose of hands-on sexual exploitation in exchange for compensation. According to Philippine Law (RA10364), this facilitation is a trafficking offense, thus this report uses the term "OSEC trafficker" or "trafficker" for brevity.

PORNOGRAPHY

Material intended to stimulate erotic feelings via explicit printed description or visual display of sexual organs or activity.

SEXTORTION

Blackmail in which sexual information or images are used to extort sexual favors and/or money from the victim.

TRAFFICKING IN PERSONS

According to the Palermo Protocol, "trafficking in persons shall mean the recruitment, transportation, transfer, harboring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labor or services, slavery or practices similar to slavery, servitude or the removal of organs. The consent of a victim of trafficking in persons to the intended exploitation set forth [above] shall be irrelevant where any of the means set forth [above] have been used. The recruitment, transportation, transfer, harboring or receipt of a child for the purpose of exploitation shall be considered trafficking in persons even if this does not involve any of the means set forth [above]." [8]

[7] The majority of victims identified in online sexual exploitation cases addressed by Philippine law enforcement have been minors, as explored further in this report. However, there have been some instances identified where adult victims have been identified along with minors, including victims who were majors at the time of rescue whose exploitation began when they were minors, and adults exploited in trafficking as defined by Philippine law. In the Philippines, these crimes are primarily charged as a trafficking offense and thus, this report did not differentiate OSEC traffickers by the age of victims.

Study Partners and Research Team

International Justice Mission (**IJM**) in partnership with the U.S. Department of State Office to Monitor and Combat Trafficking in Persons (**TIP Office**) and the Philippine Inter-Agency Council Against Trafficking (**IACAT**).

Implementing Partners

- Department of Justice (DOJ), Philippines
- Philippine National Police Women and Children Protection Center (PNP WCPC), Philippines
- National Bureau of Investigation- Anti-Human Trafficking Division (NBI-AHTRAD), Philippines
- National Center for Missing and Exploited Children, (NCMEC)
- National Crime Agency (NCA), United Kingdom
- The National Child Exploitation Crime Centre (NCECC), of the Sensitive and Specialized Investigative Services (SSIS) Branch, Royal Canadian Mounted Police (RCMP), Canada
- Federal Bureau of Investigation (FBI), United States
- Nordic Liaison Office for Police and Customs Cooperation (NLO), representing Norway, Sweden, Denmark, Finland and Iceland

Study Advisory Group

- INTERPOL
- Global Partnership to End Violence Against Children*
- Virtual Global Taskforce**
- International Centre for Missing & Exploited Children (ICMEC)

*The Global Partnership to End Violence Against Children funds a portion of IJM's collaborative casework with the Government of the Philippines to combat OSEC in Metro Cebu.

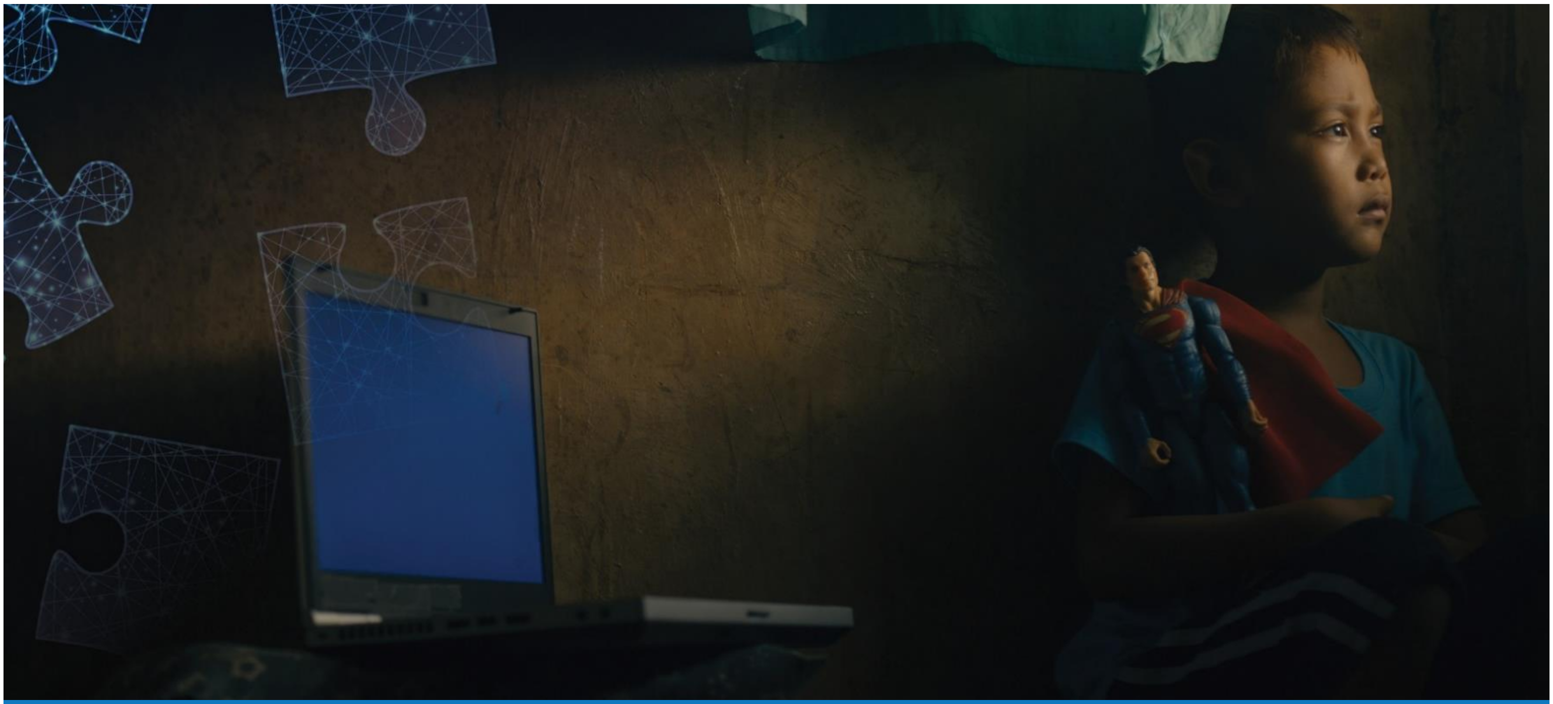
** The Virtual Global Taskforce (VGT) is an international alliance of law enforcement agencies and private sector partners working together to combat online child sexual exploitation anywhere, anytime. The VGT aims to help rescue children around the world from online sexual exploitation and identify and hold to account child sex offenders in the online environment at a global level. A full list of members can be found at www.virtualglobaltaskforce.com.

Research Team

IJM's research team contributing to this study included Rachael Jackson as research lead, Brianna Gehring as program lead and study manager, Dr. Ashley Russell as study coordinator, Dr. Kyle Vincent as contracted statistician, Nathan Sanger and Brandon Kaopuiki as law enforcement advisors, and data collectors: Kevin Bai, Astewaye Yigzaw, Eric Heintz, Chris Conrad, and Valerie Gleisberg.

Photos taken with consent. Many children pictured are actors and not victims of exploitation. Identities of victims have been obscured in order to maintain confidentiality.

This report was funded in part by a gift of the United States Government. The opinions, findings and conclusions stated herein are those of the author[s] and do not necessarily reflect those of the United States Department of State.



Executive Summary

Online Sexual Exploitation of Children (OSEC) is a complex hidden crime that is particularly challenging for the global community to measure and address. The lack of global OSEC data, the inconsistency in data collection, sharing and analysis across agencies, and the complexity of internet-facilitated crimes has made it almost impossible to accurately study and understand this crime. Yet, accurate information about its nature and scale is critical for informing and measuring the impact of stakeholder interventions to protect vulnerable children from ongoing exploitation and more effectively prevent this crime. To both set a baseline of the existing global data and catalyze future research efforts, International Justice Mission (IJM) brought together leading agencies from across multiple disciplines as well as research experts to collaboratively take on this challenge: *examine existing data sources and research methodologies in order to provide meaningful information about this crime that would be valuable for understanding its scale as well as informing interventions to combat it.*

This report presents the results of a 2019 study into the nature and scale of OSEC in the Philippines. This study was led by IJM, in partnership with the Philippine Government and a variety of stakeholders, under the U.S.-Philippine Child Protection Compact (CPC) Partnership between the U.S. Department of State Office to Monitor and Combat Trafficking in Persons and the Government of the Philippines. IJM is grateful for the extraordinary participation of the 15 partners representing governments, law enforcement, researchers, and non-governmental organizations, who generously shared their data and case histories, consulted on study methodology, and shared their expertise in the implementation and review of this study. This collaboration sets a strong foundation for future efforts to more effectively study and combat this global and local crime.

For the purposes of this study, OSEC is defined as the production, for the purpose of online publication or transmission, of visual depictions (e.g., photos, videos, live streaming) of the sexual abuse or exploitation of a minor for a third party who is not in the physical presence of the victim, in exchange for compensation.

SCOPE AND METHODS

This study examines data from across three major sources – CyberTipline reports submitted by electronic service providers (ESPs) to the National Center for Missing & Exploited Children (NCMEC), a survey of OSEC cases investigated by some of the law enforcement agencies engaged in the Virtual Global Taskforce (VGT), and the case files of OSEC cases originating in the Philippines that have been referred to or investigated by Philippine law enforcement agencies. Together, these data illuminate both the nature and scale of online sexual exploitation of children and provide a clearer understanding of the criminals and victims involved, as well as how and where crimes may be occurring.

Study partners assessed numerous methodological options before agreeing upon the approaches taken in this study. As a result, the partners selected three major research objectives to include within this study. Each objective was achieved through a separate study methodology.

1. **Estimate the baseline prevalence of internet-based child sexual exploitation (CSE) and OSEC in the Philippines**

Employ a mark-recapture methodology with data from NCMEC CyberTipline reports to estimate the number and percent of Philippine IP addresses used for CSE generally and OSEC specifically.

2. **Assess the nature of OSEC in the Philippines during the baseline time period**

Conduct an in-depth casefile review of OSEC cases investigated by Philippine law enforcement agencies, in order to gather data on the offending process and create offender and victim typologies based on previous cases.

3. **Examine the Philippines as a global hotspot for OSEC during the baseline time period**

Analyze data from global law enforcement agencies and from NCMEC CyberTipline reports that were classified as involving incidents of "online enticement" to better understand OSEC cases in the Philippines as compared to the global context.

FINDINGS

The NCMEC CyberTipline reports highlighted growth over time in the use of Philippine IP addresses for internet-based child sexual exploitation. Four key findings were identified from this data:

1. There was a consistent, sharp rise in the number of IP addresses linked to the Philippines between 2014 and 2017.
2. The estimated number/prevalence rate of IP addresses used for CSE each month grew more than 12-fold between 2014 and 2017.
3. The estimated number/prevalence rate of IP addresses used for CSE each year more than doubled between 2014 and 2017.
4. Due to inconsistencies in the quality of the data within the open-ended text fields in CyberTipline reports, it was not possible to estimate the percent of internet based CSE that is suspected to be OSEC.

The in-depth casefile review provided information on how Philippine OSEC cases were initiated, typologies of OSEC victims, customers, and traffickers, as well as information on the offending process. Twelve key findings were identified from this data:

1. The majority (64%) of Philippine OSEC cases were initiated by referrals from international law enforcement agencies.
2. The annual number of cases referred to and/or investigated by Philippine anti-trafficking units increased sharply and consistently from 2014 (1 case) to 2017 (43 cases).
3. The characteristics of OSEC victims were distinct from those of victims of establishment-based commercial sexual exploitation of children.
4. OSEC was usually a family-based crime.
5. Without intervention, the abuse usually lasted for years.
6. Customers tended to be older men.
7. Customers tended to be from Western countries, although many had traveled to or lived in the Philippines at some point in time.
8. There was an average of two traffickers per case.
9. Traffickers tended to be younger Filipina women, often family members of the victims.
10. Most criminals who got caught communicated in English.
11. The crime occurred on the surface of the internet.
12. There appears to be a financial motivation to the crime for most facilitators of OSEC.

Data on global law enforcement OSEC cases that had been referred from one country to another and NCMEC data on CyberTipline reports that were classified as involving incidents of “online enticement” were examined to understand the Philippines within a global context. Two key findings were identified from this data:

1. According to global law enforcement data, the Philippines was the largest known source of OSEC cases.
2. The Asia/Pacific region was the third largest source of “online enticement” CyberTipline reports.

Overall, the data from all three parts of this study suggest that OSEC is a serious and growing problem in the Philippines, perpetrated by a unique type of offender and affecting very young children. Due to the lack of quality data that exists on OSEC and complexity of the crime, this experimental study should be used as a catalyst for the global stakeholder community to continue prioritizing and improving data collection and analysis so we can collectively understand and effectively address this crime, as well as the impact of our interventions.

CONSIDERATIONS AND RECOMMENDATIONS

Overall, this study's findings can be used by policymakers, practitioners, and others seeking to combat OSEC by informing interventions targeting this crime. A better understanding of the nature and scope of the crime helps improve law enforcement responses and social services for survivors. Below are some initial recommendations based on the study data and the experience of the study partners, with many recommendations stemming from this research aligning with the WePROTECT Model National Response.

1. The Philippine Government should continue scaling up the staffing and budget for its anti-trafficking law enforcement units, until they reach authorized levels at a minimum.
2. International and Philippine law enforcement agencies should maintain and build on the improved relationships and communication practices that exist between them to better hold perpetrators accountable and decrease criminal impunity globally.
3. International and Philippine law enforcement agencies should ensure OSEC cases are routed to one of the Philippine anti-trafficking units (PNP WCPC and NBI-AHTRAD).
4. Government and non-government service providers should ensure a collaborative, trauma-informed, appropriate, and holistic system of care exists to address the unique needs of OSEC survivors on an individual, family, and community level.
5. Child protective measures and trauma-informed care should be implemented throughout the prosecution process of OSEC cases to protect victims from re-traumatization.
6. Technology platforms should identify and implement means for proactive detection of livestreaming OSEC.
7. Entities from across sectors should collaborate to strengthen processes to identify and report potential OSEC activity.
8. Reporting of suspected CSEM on ESP platforms should be expanded and strengthened through mandatory reporting legislation in all States and the provision of higher quality information in reports.
9. OSEC-related data owners, academics, technology designers, and OSEC experts should collaborate to conduct more research, increase our global knowledge about OSEC, as well as build the global stakeholder community's capacity to measure prevalence of the crime and impact of key interventions.
10. All stakeholders should contribute toward an increase in international and cross-sector collaboration to protect children from online exploitation.

Introduction

A DANGEROUS SIDE TO THE INTERNET

Access to the internet has brought increased opportunities to children across the globe. The internet provides access to information and ideas, learning, the global marketplace, and connections to friends and family who live far away. But, in addition to its benefits, this connection is also being used by criminals to exploit vulnerable children around the world. Child sex offenders who would prey on victims through in-person, contact abuse can now abuse children anywhere using the world wide web, and technology has created a marketplace where this abuse can now be bought and sold online.

As high-speed internet connectivity has spread across much of the globe, offenders adopted its use as an additional method through which to exploit children. This newer, technological form of exploitation provides offenders convenient access to minors from home, work, or anywhere their mobile devices can access the internet, and it has largely shielded them from law enforcement detection and intervention. Vulnerable children in developing countries – especially those with widespread internet access but insufficiently resourced justice systems – have been targeted by online offenders in similar ways as they were previously targeted by traveling offenders.

In recent years, there has been growing awareness of internet crimes against children, with child protection agencies, law enforcement, and others acknowledging a growing set of issues and working to address them.

Online crimes against children occur in many forms – sharing of abuse images, manipulating children online for abuse, sextortion, and trafficking all represent types of online crimes. However, reliable data on these crimes is lacking. Where data related to ICAC does exist, it is often in an overwhelming volume to the point where it is not able to be analyzed usefully, and much of it lacks sufficient detail to discern exactly what type of offending has occurred. Often, a full investigation is the only way of determining whether, for example, an offender identified as distributing child sexual exploitation material (CSEM) was sharing images found elsewhere online or creating them by abusing a child in their care. Given the sheer scale of reports of potential child sexual abuse material found on the platforms of electronic service providers (ESPs), full investigation of each report is impossible.

The immediate and repeated consequence of this data ambiguity is a reduced ability of ESPs, law enforcement, and others to respond effectively to specific instances of abuse. The longer-term impact is that this lack of clarity inhibits stakeholders from understanding changes in specific online crime types over time and tailoring responses to fit. Nonetheless, accurate information about the nature and scale of these crimes is critical for informing interventions by law enforcement, NGOs, industry, and others to protect vulnerable children from ongoing exploitation and more effectively prevent abuse over time.

EXAMINING OSEC

This study aims to look into the issue of OSEC, a subset of internet crimes against children. For the purposes of this study, **OSEC is defined as the production, for the purpose of online publication or transmission, of visual depictions (e.g., photos, videos, live streaming) of the sexual abuse or exploitation of a minor for a third party who is not in the physical presence of the victim, in exchange for compensation.**

This study addresses OSEC so that law enforcement, ESPs, NGOs, and other practitioners globally may have greater ability to understand and address it more fully. It is of great value for stakeholders to understand and combat all forms of internet crimes against children, and there is a growing body of work in this area. A more in-depth overview of issues associated with OSEC, related crimes, and the existing research can be found within the literature review in the next section of this report. However, while much of the existing research and interventions targeting the prevention of online crime focus on the sharing of abusive images more generally, this study aims to examine a major source of new abuse material where child victims are exploited in situations of often ongoing and violent abuse, with traffickers feeding the demand for new material from customers around the world.

Over the past decade, law enforcement agencies have identified a global increase in known cases of exploitation with a commercial element.[9] In OSEC cases, typically, an offender, referred to in this report as an OSEC customer, sends payment via a money transfer agency (MTA) to the OSEC trafficker, who has access to children and abuses or exploits them to produce child sexual exploitation material (CSEM). This material is often transmitted via live-streaming video communications platforms. These acts constitute trafficking in persons, as defined by the Palermo Protocol.[10] The economic payment for the CSEM or exploitative display is what makes this crime unique and distinct from other common, but non-commercial, forms of internet crimes against children.

Livestreaming and creating CSEM on-demand allow the remote OSEC customer to take an active role in creating the visual display of child sexual abuse and exploitation by directing the actions of the trafficker and exploited children. Major ESPs with livestreaming functionality typically do not monitor such data streams for possible CSEM. Because the livestream does not, by nature, result in a stored image or video file – the most commonly detected indicators of ICAC offenses – detection methods in common use do not typically recognize livestreaming OSEC. This results in the majority of instances remaining unreported. The evidence that does exist is often spread across different platforms including social media apps, MTAs, and computers/mobile devices, making it difficult for ESPs, law enforcement, and others to identify when this crime occurs.

By focusing this research effort on OSEC specifically, stakeholders can target the most effective interventions to combat this particular form of abuse as well as prioritize action in source countries and on platforms through which the crime is transmitted. For instance, while a campaign that educates students in schools about the dangers of self-producing images and sexting may be very effective in an area where these issues are common, that same campaign will have little to no effect at protecting children in a community where OSEC is prevalent and

[9] Based on conversations with stakeholders working in the field.

[10] Protocol to Prevent, Suppress and Punish Trafficking in Persons. Especially Women and Children, Supplementing the United Nations Convention Against Transnational Organized Crime, U.N. Doc. A/53/383 (2000) [hereinafter Palermo Protocol], available at https://www.ohchr.org/en/professionalinterest/pages/protocoltraffickinginpersons.aspx

minors are trafficked by an adult rather than generating abuse materials themselves or engaging with abusers directly online.

Thus, to understand OSEC better, this study closely examines the available information from across partners in the law enforcement and child protection space,[11] illuminating a crime that occurs in the shadows and providing stakeholders with valuable information on where and how this crime occurs, with a particular focus on investigations of OSEC originating from the Philippines for the reasons laid out below.

GLOBAL COLLABORATION AND PHILIPPINE FOCUS

Data on OSEC crimes is limited and is spread across disparate sources, making it difficult for the global community to effectively measure the full scale of the crime. Thus, International Justice Mission (IJM) brought together leading agencies working in this area from across disciplines as well as research experts to collaboratively take on this challenge: examining existing data sources and research methodologies available to determine how to provide meaningful information about this crime that would be valuable for understanding its scale as well as informing interventions to combat it. These agencies worked together to identify and examine data that exists from across sources and collaboratively developed an innovative approach to studying this issue. The study team includes partners from law enforcement agencies across the globe, researchers, child protection NGOs, and government agencies. Together, these partners assessed several approaches and identified several methodologies that would be able to provide valuable data to the community of stakeholders working on this issue.

The study examines data from across disparate sources – an analysis of CyberTipline reports submitted by ESPs to the National Center for Missing & Exploited Children (NCMEC), a survey of cases referred from some of the law enforcement agencies engaged in the Virtual Global Taskforce (VGT), and a deep dive case file review into cases of OSEC originating in the Philippines that have been investigated by Philippine law enforcement agencies. Together, these data illuminate both the nature and scale of online sexual exploitation of children and provide a clearer understanding of the criminals and victims involved and how and where crimes may be occurring.

This study looks at global data where possible, but narrows into the Philippines specifically because IJM works with the Government of the Philippines to support efforts to combat OSEC, and this study is a part of IJM's programming efforts there. Live-streaming OSEC is not unique to the Philippines, but it is believed to be more prevalent in the Philippines than in other countries. This is likely due to the combined impact of numerous enabling factors, including but not limited to: a historic commercial sex industry and underground reputation as a sex trafficking source country and destination for traveling sex offenders; a robust money remittance infrastructure; widespread, inexpensive internet access through broadcast-capable mobile devices; and English language proficiency throughout all social strata at levels which are much higher than other developing countries.

The Philippine Government has been open to cooperating with foreign governments, NGOs, and domestic stakeholders to respond to this emerging threat to children, equipping law enforcement, courts, and social services with increasing means to respond. Thus, the Government has investigated and responded to hundreds of OSEC cases, rescuing children from ongoing situations of abuse and arresting traffickers. In 2017, the Government of the Philippines

[11] A full list of study partners is documented on page 10.

entered into the U.S.-Philippines Child Protection Compact (CPC) Partnership with the U.S. Department of State Office to Monitor and Combat Trafficking in Persons. The CPC committed resources from both governments toward a plan to increase protection of children from OSEC and labor trafficking. International Justice Mission (IJM) is an implementing agency of the CPC and led the implementation of this research study as part of the CPC. This study is commissioned to understand the nature and scale of OSEC in the Philippines and more broadly to identify key learnings in the efforts to combat it both locally and globally.

IJM has supported the Government of the Philippines in responding to child sex trafficking for almost 20 years. Over this period, the response to the exploitation of minors in establishment and street-based trafficking significantly improved. Between 2006 and 2016, IJM identified reductions in the prevalence of child sex trafficking of between 79% and 86% in target cities with the largest commercial sex markets, and in 2016, the Government was ranked on Tier 1 of the TIP Office's annual TIP report – the first nation in the region to achieve a Tier 1 ranking – a ranking that is still maintained as of 2019.

From 2011 through the end of 2019, IJM's program has supported the Philippines in responding to 171 cases of OSEC, resulting in 571 victims rescued, 229 suspects charged, and 76 convictions. An in-depth analysis of a portion of these cases provides stakeholders from other regions with valuable information on how the crime occurs and the demographics of offenders as well as victims to prepare others to address these issues as well.

STUDY SCOPE AND OVERVIEW OF COMPONENTS

The primary purpose of the study is to assess the nature and scale of OSEC in the Philippines. IJM's standard approach to impact evaluation for each program includes baseline and endline measurements of the prevalence of the targeted crime to determine change over time. However, in this instance, an effective approach to measuring prevalence of OSEC in the Philippines was not able to be identified due to the hard to reach impacted population, scarcity of data related specifically to OSEC, and fragmented nature of data that do exist. Thus, IJM brought together research experts and leading agencies working in this area from across disciplines to collaboratively examine existing data sources and research methodologies. Together, these partners designed an approach that aims to measure the scale of the crime and provide valuable information to stakeholders engaged in combatting it.

The study partners determined that, given the data limitations present, the results of measurements of prevalence would be stronger if they were triangulated with other disparate data sources to give the field a better sense of how the crime is changing over time. For example, if a change in a prevalence measurement was compared with case file data correspondingly showing changes in the price of a show (an indicator of OSEC supply) or the use of advanced anonymization techniques (an indicator of ease of offending), the combined data would make a stronger case for changes in the prevalence of the crime.

As a result of these discussions, the study partners selected three major research objectives to include within this study. Each objective was achieved through a separate study methodology. (See the Methodology section for details on each method.)

1. **Estimate the baseline prevalence of internet-based child sexual exploitation (CSE) and OSEC in the Philippines**
   Employ a mark-recapture methodology with data from NCMEC CyberTipline reports to estimate the number and percent of Philippine IP addresses used for CSE generally and OSEC specifically.

2. **Assess the nature of OSEC in the Philippines during the baseline time period**
   Conduct an in-depth casefile review of OSEC cases investigated by Philippine law enforcement agencies, in order to gather data on the offending process and create offender and victim typologies based on previous cases.

3. **Examine the Philippines as a global hotspot for OSEC during the baseline time period**
   Analyze data from global law enforcement agencies and from NCMEC CyberTipline reports that were classified as involving incidents of "online enticement" to better understand OSEC cases in the Philippines as compared to the global context.

The study team chose the years 2010 through 2017 as the baseline time period for several reasons. First, all stakeholders recognized that 1) there have been significant changes in the quality of OSEC-relevant data and the ways they have been collected over the past decade, and 2) there are likely to be many more changes in these data over the coming years, complicating comparability of baseline and endline results. The team, therefore, wanted to capture multiple years of data in an attempt to see how past changes in the environment, such as changes in ESP reporting and government focus on the issue, impacted data. Second, the year 2010 was chosen as the beginning of this time period because it is the main year in which OSEC cases began to be identified within the Philippines (with only a few outliers investigated prior to 2010). Finally, the year 2017 was selected as the final year because at the time of methodology development, it was the latest year for which CyberTipline data were available.

This study represents a learning process and the efforts of committed individuals across the child protection space to better understand a hidden and complex crime. The methodologies that are implemented in this report are an imperfect but critical start to explaining this difficult-to-trace crime. We have also identified suggestions for further research and stronger data collection so that future efforts may be able to track progress in combatting this crime and more effectively inform efforts going forward. It is the hope of the partners involved that the information included in this report is valuable and ultimately helpful for the protection of children.

Literature Review

DEFINING OSEC

The sexual exploitation of children online is a global issue with an ever-increasing scope due to the rise in technology and internet connectivity around the world. Online abuse can be identified in a variety of forms;[12] therefore, it is important to define what crimes are considered OSEC and what crimes are similar, yet not considered trafficking. Under Philippine law, OSEC conduct falls within the broad category of trafficking in persons crimes. Other forms of trafficking in persons include non-sexual labor trafficking, non-commercial child sexual exploitation, and adoption for exploitative purposes. Other types of internet crimes against children – such as CSEM possession and distribution – are not considered trafficking in persons offenses.

The lack of standardization across terms referencing sexual exploitation and sexual abuse of children led to the establishment of the Interagency Working Group,[13] bringing together stakeholders to compile the various terms and phrases and provide universal definitions to key terms, known as the Luxembourg Guidelines.[14] The guidelines address the various legal definitions, non-binding instruments that use the term, considerations of how the term is used, conclusions on how best to use the term, and descriptions of terms that are similar in nature. Key terms addressed in the guidelines were chosen based on a variety of factors such as laws within international or regional treaties, terms used within context or for conduct of exploitation or abuse of children, or terms that create misunderstanding among stakeholders.[15]

In the Luxembourg Guidelines, many of the individual components of OSEC are defined under “online child sexual exploitation” and “live online child sexual abuse.” For example, the term “online child sexual exploitation” references the specific use of the internet to facilitate exploitation. The term “live online child sexual abuse”, while referencing both commercial and non- commercial use, has been known for “cases where it has been set up as a proper business with the only apparent objective being to make money out of the sexual exploitation of the children involved.”[16] One type of abuse, live streaming, typically involves content of coerced or forced abuse of a child in real time through information and communication technology (ICT), with either the trafficker manipulating the abuse or the customer directing the abuse.[17] Live streaming has been referred to by a variety of terms such as “pay-per-view,” “on-demand child sexual abuse,” or “made to order child sexual abuse.”[18]

The terms child sexual exploitation material (CSEM) and child sexual abuse material (CSAM) can both be included under the umbrella of OSEC when the trafficker has produced the material and there is an exchange of compensation. CSEM is a broad term that encompasses abusive material as well as material with sexualized content, while CSAM is a narrowly defined subset of material specific to the depiction of abuse.[19] CSEM/CSAM is widely discussed throughout

[12] ECPAT International (2018). “Trends in Online Child Sexual Abuse Material”. Retrieved from https://www.ecpat.org/wp-content/uploads/2018/07/ECPAT-International-Report-Trends-in-Online-Child-Sexual-Abuse-Material-2018.pdf

[13] The Interagency Working Group included representatives from African Committee on the Rights and Welfare of the Child, Child Rights Connect, Council of Europe Secretariat, ECPAT, Europol, INHOPE – The International Association of Internet Hotlines, Instituto Interamericano del nino, la nina y adolescents (OEA), International Centre for Missing and Exploited Children, International Labour Office, International Telecommunication Union, INTERPOL, Office of the United Nations High Commissioner for Human Rights, Plan International, Save the Children International, Special Representative of the United Nations Secretary General on Violence against Children, United Nations Committee on the Rights of the Child, United Nations Special Rapporteur on the sale of children, child prostitution and child pornography, United Nations Children’s Fund (UNICEF).

[14] ECPAT Luxembourg/ECPAT International (2016). “Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse”. Retrieved from http://cf.cdn.unwto.org/sites/all/files/docpdf/terminologyguidelines.pdf

[15] *Id.*

[16] *Id.*

[17] *Id.*

[18] Ramiro, L. S., Martinez, A. B., Tan, J. R. D., Mariano, K., Miranda, G. M. J., & Bautista, G. (2019). Online child sexual exploitation and abuse: A community diagnosis using the social norms theory. *Child Abuse & Neglect*, *96*. https://doi-org.proxy.lib.fsu.edu/10.1016/j.chiabu.2019.104080

[19] ECPAT Luxembourg/ECPAT International (2016). “Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse”. Retrieved from http://cf.cdn.unwto.org/sites/all/files/docpdf/terminologyguidelines.pdf

literature focused on internet crimes against children, but caution is advised when conflating these terms with OSEC specifically. Once predominantly commercial, this is no longer the case for the distribution of CSEM/CSAM. INHOPE's 2014 data indicates that 91% of the CSAM that they analyzed or processed were non-commercial.[20] Instead of being sold or exchanged for financial gain, they are shared among like-minded individuals at no cost.[21] The exchange of CSAM without compensation is seen across discussion boards, websites, and peer to peer exchange sites. For example, instead of paying for access to the exchange sites or discussion boards with CSEM/CSAM, admission maybe granted through uploading new abuse material.[22]

Crimes that share similarities to OSEC but fall outside of the definition include sextortion and grooming, also known as online enticement. Sextortion is defined as "blackmailing of an individual using self-generated materials to extort sexual favors, money, or other benefits from her/him under the threat of sharing the material beyond the consent of the depicted person."[23] The threat of sharing the material online or to family can be used to manipulate the individual into meeting more demands.[24] Minors engaged in "sexting," self-generated content typically used to flirt or within a romantic relationship, are particularly vulnerable if the images or videos are shared with the wrong person. Grooming is described as "a practice by means of which an adult 'befriends' a child (often online, but offline grooming also exists and should not be neglected) with the intention of sexually abusing her/him." [25]

PREVALENCE AND LOCATION ESTIMATES

The increase in availability and access to the internet has been a contributing factor in OSEC across the globe. Currently an estimated 2.5 billion people globally have access to the internet,[26] with growth expected to continue over time. No true measure of OSEC prevalence has been established. Rather, research has mainly focused on estimating the number of online offenders, victims that can be identified, and reports to law enforcement, as well as identifying countries where CSAM/CSEM material is hosted and broadcasted. The most common estimate of offenders is 750,000 individuals worldwide, an estimate produced by the UN and the FBI.[27] Terre des Hommes conducted a study where investigators, under the guise of a young Filipina, interacted with 20,127 predators in public chat rooms over a 10-week period and specifically focused on customers acknowledging that they were purchasing pre-pubescent Filipina children.[28] During the study, researchers were able to identify and locate 1,000 predators across 71 countries.[29] Other studies with a location-specific focus have found similar results. In 2017, INHOPE's hotline data identified 70 countries where CSAM was hosted online.[30] The INHOPE hotline identified the United States, Netherlands, Russian Federation, France, and Canada as the top five countries hosting CSAM.[31] In a study by INTERPOL, media from the International Child Sexual Exploitation (ICSE) database categorizes the children in CSAM images as being identified by law enforcement or unidentified. The study found 72 countries recorded as a place

[20] INHOPE (2015), "Worldwide commercial hosting in 2014". Retrieved from http://88.208.218.79/tns/resources/statistics-and-infographics/statistics-and-infographics-2014.aspx

[21] *Id.*

[22] Mitchell, K. J., Jones, L. M., Finkelhor, D., & Wolak, J. (2014). Trends in unwanted online experiences and sexting.

[23] ECPAT Luxembourg/ECPAT International (2016). "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse". Retrieved from http://cf.cdn.unwto.org/sites/all/files/docpdf/terminologyguidelines.pdf

[24] *Id.*

[25] *Id.*

[26] Statistics and Market Data on Online Demographics & Use. Retrieved from https://www.statista.com/markets/424/topic/537/demographics-use/

[27] Terre des Hommes (2013). Netherlands, November 2013 *Webcam child sex tourism – becoming sweetie: A novel approach to stopping the global rise of webcam child sex tourism,* 113 Retrieved from www.terredeshommes.nl.

[28] *Id.*

[29] *Id.*

[30] INHOPE (2018), "2017 Annual Report". Retrieved from http://88.208.218.79/tns/resources/annual-reports.aspx

[31] *Id.*

of abuse. Eastern European and Southeast Asian countries were found to be the most prominent places of abuse within the 10.7% of media that recorded a suspected country of abuse and the children remain unidentified by law enforcement. North American and Western European countries were the most prominent places of abuse within the 55% of media files that identified the children in the images.[32] Researchers suggest increased identification of place of abuse in identified media is more likely to be based on better victim identification and reporting policies in those countries with identified media and not necessarily on a higher prevalence of CSAM/CSEM. On the other hand, lack of identified media does not indicate a lack of abuse in a country and could indicate locations with an increased need for training or connections to the database.

The production and sharing of CSAM/CSEM, while not deemed trafficking unless there is financial compensation, is the closest proxy indicator to estimating the number of victims. While the Terre des Hommes study was not primarily focused on identifying child victims, researchers did examine 84 public websites offering webcam sex performances resulting in over 200 individuals selling performances and roughly 30% of the websites have children involved.[33] In another study, the Canadian Center for Child Protection identified 46,859 images of unique children with 78.3% under the age of 12.[34] INHOPE's 2017 hotline data included 87,930 reports with a total of 259,016 images and videos identified.[35] Of the content identified by the INHOPE hotlines, 47% of the content are classified as international illegal by INTERPOL criteria and 82% of the subjects in content classified as CSAM are between zero and thirteen years old.[36]

DESCRIPTIONS OF TRAFFICKERS, CUSTOMERS, AND VICTIMS

Terre des Hommes research identified three types of OSEC traffickers/facilitation in the Philippines – a family member or friend, "self-facilitated" material, and cybersex "dens." Multiple studies support the finding of a close friend of family member identified as the OSEC trafficker.[37,38,39] A NCMEC (2015) study on CSAM, where both child and abuser were known, found 74% of cases of CSAM traded or distributed were facilitated by someone within the child's "circle of trust," such as a family member, guardian, or family friend.[40] Family or friends exploiting children seek to excuse their behavior by viewing these online offenses as less harmful than contact offense.[41,42] Parents, if not the trafficker themselves, tend to be aware of the activities their child is engaging in but do not get involved or stop the activities as there is financial gain for them.[43]

[32] Child, O.U.V.I (2018). Towards a Global Indicator: On Unidentified Victims in Child Sexual Exploitation Material. Retrieved from https://www.ecpat.org.uk/towards-a-global-indicator-on-child-sexual-exploitation-material

[33] *Id.*

[34] Rimer, J. R. (2019). "In the street they're real, in a picture they're not": Constructions of children and childhood among users of online child sexual exploitation material. *Child Abuse & Neglect*, *90*, 160–173. https://doi-org.proxy.lib.fsu.edu/10.1016/j.chiabu.2018.12.008

[35] INHOPE (2018), "2017 Annual Report". Retrieved from http://88.208.218.79/tns/resources/annual-reports.aspx

[36] *Id.*

[37] Terre des Hommes (2013). Netherlands, November 2013 *Fullscreen on View – An Exploratory Study on the Background and Psychosocial Consequences of Webcam Child Sex Tourism in the Philippines.* Retrieved from www.terredeshommes.nl.

[38] Child, O.U.V.I (2018). Towards a Global Indicator: On Unidentified Victims in Child Sexual Exploitation Material. Retrieved from https://www.ecpat.org.uk/towards-a-global-indicator-on-child-sexual-exploitation-material

[39] National Center for Missing & Exploited Children (2015), "Child Pornography Offending: Analysis of Data from NCMEC" (presentation delivered at 27th Annual Crimes against Children Conference, Dallas, Texas, USA, 10-13 August 2015).

[40] *Id.*

[41] Ramiro, L. S., Martinez, A. B., Tan, J. R. D., Mariano, K., Miranda, G. M. J., & Bautista, G. (2019). Online child sexual exploitation and abuse: A community diagnosis using the social norms theory. *Child Abuse & Neglect*, *96*. https://doi-org.proxy.lib.fsu.edu/10.1016/j.chiabu.2019.104080

[42] Terre des Hommes (2013). Netherlands, November 2013 *Fullscreen on View – An Exploratory Study on the Background and Psychosocial Consequences of Webcam Child Sex Tourism in the Philippines.* Retrieved from www.terredeshommes.nl.

[43] Ramiro, L. S., Martinez, A. B., Tan, J. R. D., Mariano, K., Miranda, G. M. J., & Bautista, G. (2019). Online child sexual exploitation and abuse: A community diagnosis using the social norms theory. *Child Abuse & Neglect*, *96*. https://doi org.proxy.lib.fsu.edu/10.1016/j.chiabu.2019.104080

Terre des Hommes identified the “self-facilitating” victims as a second group. There is ambiguity around the phrase “self-facilitating” or “self-generated” in terms of what is considered OSEC. The Terre des Hommes study described older teenagers sending material to foreign customers. By definition, the teenagers are minors and legally considered trafficked. This does not take into consideration any grooming that might have taken place or manipulation to self-generate the material. As mentioned before, “self-generated” photos do not always indicate OSEC. There are cases where the children are too young to be facilitating the financial transaction and there is an adult involved, while not known to the customer.[44,45] While not as common as the first two groups, there are set ups deemed as “cybersex dens”[46,47] where multiple people are held and abused for years to audiences across the globe. Fieldwork has found dens to be run by organized crime groups as well as foreign nationals.[48] Other establishments like “dens” are internet and pisonet cafes. These cafes provide easy access to the internet that, while there is an attempted from managers to monitor the contents and activities conducted, have been known to be used for grooming and CSEM[49].

OSEC customers and child sexual abusers are often confused as pedophiles, however, OSEC customers “include a much greater number of people who are willing to engage in web cam sex tourism if the opportunity is present, but who may not meet the clinical criteria for pedophilia.”[50] Pedophilia is a clinical diagnosis where “the presence of sexual fantasies, urges, or behaviors that involve sexual activity with a prepubescent child last for a period of at least six months.”[51] One study estimated less than 5% of adult men globally are considered pedophiles,[52] while another study focused on a university sample that identifies around 20% of the males in the sample have sexual interest in prepubertal children.[53] A study of the general population in Germany found less than 0.1% of the 8,718 sample to have pedophilic preferences, whereas 4.1% had sexual fantasies of prepubescent children and 3.2% conducted sexual offences against prepubescent children.[54] While pedophiles may be in search of CSEM, OSEC customers are not limited to those meeting the criteria of pedophilia.

In addition to the relationship between online child sexual abuse and pedophilia, research has examined the differences between those who are known to be only online offenders, compared to those who are known to be only contact offenders or dual online and contact offenders.[55] In a rapid assessment of literature that provided characteristics of online offenders, most samples were based on perpetrators who had been prosecuted or at least identified by law enforcement.[56]

[44] Child, O.U.V.I (2018). Towards a Global Indicator: On Unidentified Victims in Child Sexual Exploitation Material. Retrieved from https://www.ecpat.org.uk/towards-a-global-indicator-on-child-sexual-exploitation-material

[45] Terre des Hommes (2013). Netherlands, November 2013 *Fullscreen on View – An Exploratory Study on the Background and Psychosocial Consequences of Webcam Child Sex Tourism in the Philippines.* Retrieved from www.terredeshommes.nl.

[46] *Id.*

[47] Ramiro, L. S., Martinez, A. B., Tan, J. R. D., Mariano, K., Miranda, G. M. J., & Bautista, G. (2019). Online child sexual exploitation and abuse: A community diagnosis using the social norms theory. *Child Abuse & Neglect*, *96*. https://doi-org.proxy.lib.fsu.edu/10.1016/j.chiabu.2019.104080

[48] Terre des Hommes (2013). Netherlands, November 2013 *Fullscreen on View – An Exploratory Study on the Background and Psychosocial Consequences of Webcam Child Sex Tourism in the Philippines.* Retrieved from www.terredeshommes.nl.

[49] Ramiro, L. S., Martinez, A. B., Tan, J. R. D., Mariano, K., Miranda, G. M. J., & Bautista, G. (2019). Online child sexual exploitation and abuse: A community diagnosis using the social norms theory. *Child Abuse & Neglect*, *96*. https://doi-org.proxy.lib.fsu.edu/10.1016/j.chiabu.2019.104080

[50] Terre des Hommes (2013). Netherlands, November 2013 *Webcam child sex tourism – becoming sweetie: A novel approach to stopping the global rise of webcam child sex tourism,* 19 Retrieved from www.terredeshommes.nl.

[51] *Id.*

[52] *Seto M. C. (2009)* Pedophilia*. Annual Review of Clinical Psychology 5:391–407.*

[53] Briere, John, PhD., Runtz, Marsha, M.A. (1989). “University males’ sexual interest in children: Predicting potential indices of “pedophilia” in a nonforensic sample”. pg. 71
University of Southern California School of Medicine.

[54] Dombert, Schmidt, Banse, Briken, Hoyer, Neutze and Osterheider (2016), “How Common is Men’s Self-Reported Sexual Interest in Prepubescent Children?”, accessed August 2019, https://www.ncbi.nlm.nih.gov/pubmed/26241201

[55] DeMarco, J., Sharrock, S., Crowther, T., & Barnard, M. (2018). Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation. *NatCen Social Research Final Report*.

[56] *Id.*

Of this literature, online-facilitated offenders tend to be male from a Caucasian or European background.[57] They are also more likely to have higher education, employment, and are more technologically savvy.[58] Compared to contact offenders, online offenders are less likely to have prior criminal backgrounds, convictions, or history of anti-social behavior.[59] The age of offenders ranges from mid-twenties to fifties and sixties, with no significant difference in ages across online-only and contact offenders.[60] Similar to how parents seek to excuse their facilitation of OSEC, there is research to suggest that the online nature of the abuse enables offenders to disassociate CSEM from actual harm of children.[61] For example, customers would often refer to the children in images as "them," "not real," or "just pictures" and note their lack of intention to abuse children in real life.[62]

Research on CSAM victim profiles examine a few key characteristics including, age, sex, severity of abuse/exploitation, the number of victims depicted, and the type of production. Age ranges have found exploitation of infants to pubescent children, with some children being identified over time at various stages.[63] Studies have found that images of younger victims are increasingly more disturbing and severe.[64,65] For example, the International Watch Foundation's (IWF) 2018 annual report found that "35% of the imagery showing children appearing to be aged 10 or younger was assessed as being Category A, compared to 16% of the imagery showing children aged 11-17," where Category A is defined by the "showing of sexual activity between adults and children including rape or sexual torture."[66] The vast majority of research finds female victims more often than male victims,[67] however male victims are not uncommon amongst CSAM/CSEM. IWF identified 17% of victims to be boys and 4% showcasing victims of both genders.[68] Even when a victim is removed from exploitation, the longstanding effects of online exploitation is unknown. The IWF annual report highlights the repeat victimization and long-term abuse of children in the story of Olivia.[69] "We see Olivia every day—five years after she was rescued. To show exactly what 'repeat victimization' means, we counted the number of times we saw Olivia's image online during a three-month period. We saw her at least 347 times. On average, that's five times each and every working day."[70]

COMBATTING OSEC

Recommendations throughout literature mostly focus on prevention through internet safety education and awareness about the harm and consequences around online sexual abuse.[71] Many organizations have promoted educational campaigns focused on safe internet practices to parents and children to decrease vulnerability. Other general awareness efforts like the

[57] *Id.*

[58] Seto, M. C., Buckman, C., Dwyer, R. G., & Quayle, E. Production and Active Trading of Child Sexual Exploitation Images Depicting Identified Victims: NCMEC/Thorn Research Report. *Alexandria, VA: National Center for Missing & Exploited Children*.

[59] DeMarco, J., Sharrock, S., Crowther, T., & Barnard, M. (2018). Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation. *NatCen Social Research Final Report*.

[60] *Id.*

[61] Rimer, J. R. (2019). "In the street they're real, in a picture they're not": Constructions of children and childhood among users of online child sexual exploitation material. *Child Abuse & Neglect*, *90*, 160–173. https://doi-org.proxy.lib.fsu.edu/10.1016/j.chiabu.2018.12.008

[62] *Id.*

[63] Child, O.U.V.I (2018). Towards a Global Indicator: On Unidentified Victims in Child Sexual Exploitation Material. Retrieved from https://www.ecpat.org.uk/towards-a-global-indicator-on-child-sexual-exploitation-material

[64] Canadian Centre for Child Protection (2016). "Child Sexual Abuse Images on the Internet: A Cybertip.ca Analysis." Canada

[65] Child, O.U.V.I (2018). Towards a Global Indicator: On Unidentified Victims in Child Sexual Exploitation Material. Retrieved from https://www.ecpat.org.uk/towards-a-global-indicator-on-child-sexual-exploitation-material

[66] Internet Watch Foundation. (2018). Annual Report. Retrieved from https://www.iwf.org.uk/report/2018-annual-report

[67] Child, O.U.V.I (2018). Towards a Global Indicator: On Unidentified Victims in Child Sexual Exploitation Material. Retrieved from https://www.ecpat.org.uk/towards-a-global-indicator-on-child-sexual-exploitation-material

[68] Internet Watch Foundation. (2018). Annual Report. Retrieved from https://www.iwf.org.uk/report/2018-annual-report

[69] Olivia is a pseudonym.

[70] Internet Watch Foundation. (2018). Annual Report. Retrieved from https://www.iwf.org.uk/report/2018-annual-report

[71] Bouché, V. (2015). A report on the use of technology to recruit, groom and sell domestic minor sex trafficking victims.

Dunkelfeld project and Stop It Now cater prevention tactics to the potential offenders by promoting seeking help before offending.[72]

Another type of recommendation includes disruption tactics to stop customers before or in the middle of their involvement with CSAM/CSEM. Google and Microsoft have implemented blocking efforts as a disruption tactic and found that it reduced the number of web-based searches for abuse images by 67% compared to a non-blocking search engine.[73,74] Microsoft also initiated pop up messages when search terms are linked to illegal conduct.[75] PhotoDNA, created by Microsoft, is used to help reduce the proliferation of CSAM. PhotoDNA is an image matching technology and uses a mathematical algorithm to create a unique image signature that can be compared against known abuse images. The use of PhotoDNA has led to a disruption of over 4 million images.[76]

Terre des Hommes recommended shifting from reactive law enforcement policies to proactive investigative techniques.[77] Researchers determined that customers' perceptions of risk are low, based on the ease with which they were able to convince customers in their study to reveal themselves and effectively be identified. Proactive investigation is expected to have a deterrent effect, increasing perceived risk of participating in WCST and reducing the number of victims.[78] THORN actively conducts an online deterrence program by "communicating directly with people searching for CSAM, disrupting their sense of anonymity and encouraging them to seek help." So far, the program has seen over 2.8 million visitors and more than 168,000 instances where individuals chose to seek help after contact with the deterrence program.[79]

While safe internet practices by children and risk awareness of parents can impact vulnerability of potential victims of CSAM in general, and disruption tactics focused on the customer can intervene, more research is needed to proactively combat the traffickers of OSEC. Like commercial sexual exploitation of those in person, the facilitation and distribution of these materials (pictures, videos, live stream, etc.) needs to be deterred through an increase in risk and a decrease in anonymity. It is unknown if there is any research that highlights efforts to deter the traffickers.

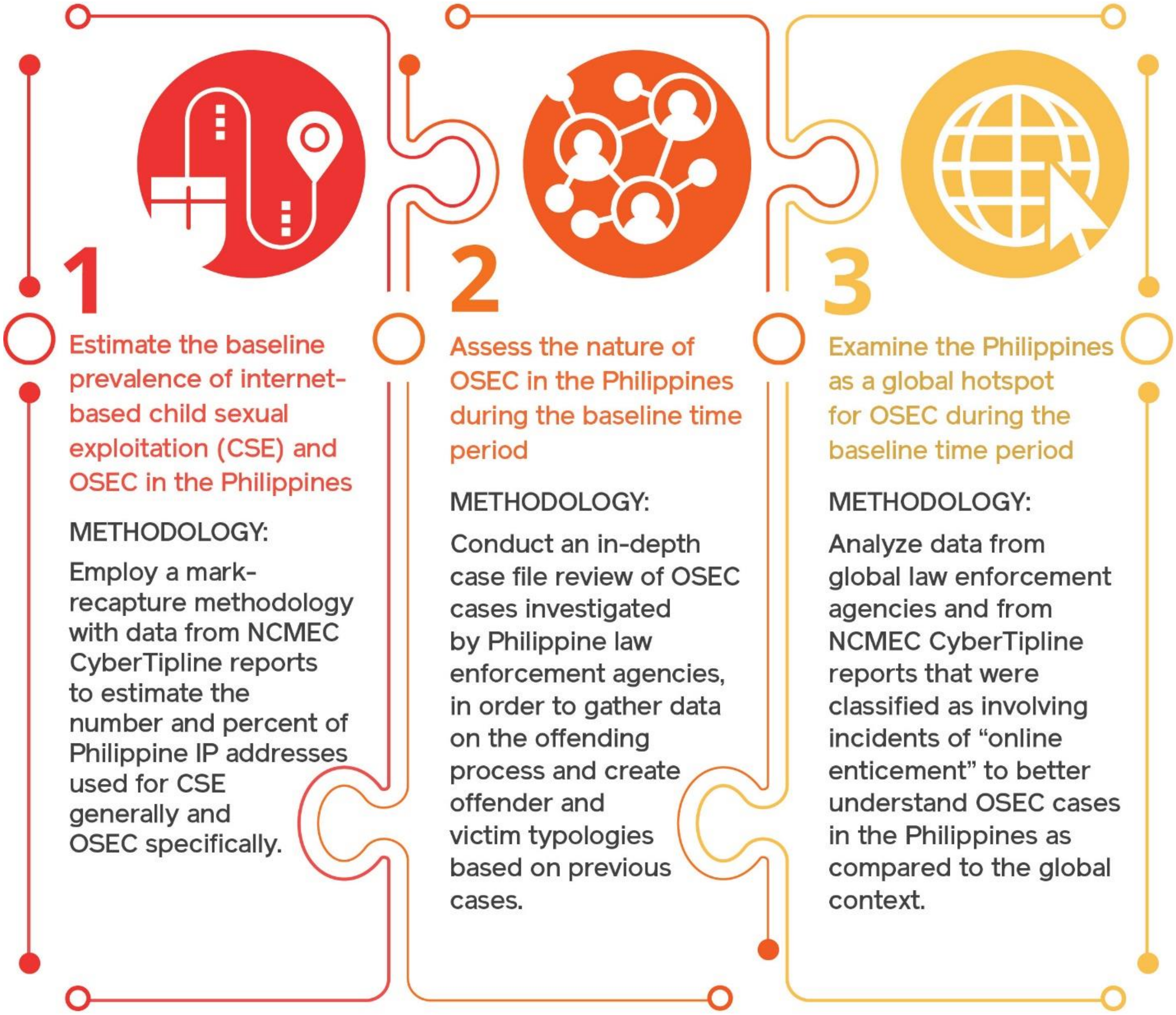
Overall, most research available focuses on components of OSEC, such as the production of CSAM/CSEM or live streaming of abuse, but there are very few studies that capture the full extent of the crime including both production of, and compensation for, these materials. The aim of this current study is to add to the literature a more in-depth analysis of this particular crime, addressing the nature of the crime, the global reach traffickers can obtain through the internet, and recommendations for effective intervention.

[72] Quayle, E., & Koukopoulos, N. (2018). Deterrence of online child sexual abuse and exploitation. *Policing: A Journal of Policy and Practice*.
[73] *Id.*
[74] Steel, C. M. (2015). Web-based child pornography: The global impact of deterrence efforts and its consumption on mobile platforms. *Child abuse & neglect*, *44*, 150-158.
[75] Quayle, E., & Koukopoulos, N. (2018). Deterrence of online child sexual abuse and exploitation. *Policing: A Journal of Policy and Practice*.
[76] THORN (2015). *The Use of Technology to Recruit, Groom and Sell Domestic Minor Sex Trafficking Victims.* Retrieved from https://www.thorn.org/resources-and-research/
[77] Terre des Hommes (2013). Netherlands, November 2013 *Webcam child sex tourism – becoming sweetie: A novel approach to stopping the global rise of webcam child sex tourism,* 19 Retrieved from www.terredeshommes.nl.
[78] Terre des Hommes (2013). Netherlands, November 2013 *Fullscreen on View – An Exploratory Study on the Background and Psychosocial Consequences of Webcam Child Sex Tourism in the Philippines.* Retrieved from www.terredeshommes.nl.
[79] THORN.(n.d). Retrieved from https://www.thorn.org/deterrence-prevent-child-sexual-abuse-imagery/

Methodology

This study sought to accomplish three major research objectives to assess the nature and scale of OSEC in the Philippines, with each objective being achieved through a separate study methodology. This section includes a summary of the methods used under each objective.

Figure 1: Research Objectives and Methodology



1

Estimate the baseline prevalence of internet-based child sexual exploitation (CSE) and OSEC in the Philippines

METHODOLOGY:

Employ a mark-recapture methodology with data from NCMEC CyberTipline reports to estimate the number and percent of Philippine IP addresses used for CSE generally and OSEC specifically.

2

Assess the nature of OSEC in the Philippines during the baseline time period

METHODOLOGY:

Conduct an in-depth case file review of OSEC cases investigated by Philippine law enforcement agencies, in order to gather data on the offending process and create offender and victim typologies based on previous cases.

3

Examine the Philippines as a global hotspot for OSEC during the baseline time period

METHODOLOGY:

Analyze data from global law enforcement agencies and from NCMEC CyberTipline reports that were classified as involving incidents of "online enticement" to better understand OSEC cases in the Philippines as compared to the global context.

ESTIMATING THE BASELINE PREVALENCE OF INTERNET-BASED CSE AND OSEC IN THE PHILIPPINES

One objective of this study was to estimate the baseline prevalence of internet-based child sexual exploitation, generally, and OSEC specifically, in the Philippines between 2010 and 2017. This section includes a summary of the methods used in the analysis of NCMEC CyberTipline reports. For a more detailed description of the methods, see Appendix A.

The Conceptual Framework

The term "prevalence" refers to the percent of units within a population that has a specific characteristic during a specific time period. Often the population of interest is a group of people, but it can be any group of related objects. Due to significant challenges in collecting accurate data within the human populations of interest in this study (either children who are OSEC victims or adults who are OSEC traffickers[80]), the study team decided to use Philippine-based IP addresses as the population of interest. Thus, the "prevalence" statistic for this study would be the estimated percent of all Philippine-based IP addresses associated with suspected OSEC activity.

This statistic is similar to those used in other human trafficking studies that have measured the percent of worksites that use bonded labor or the percent of brothels that offer child sexual exploitation, in that it considers the location of the exploitation as the unit of measure. Unlike those studies, however, this study is looking at an electronic network's "locations" instead of a geographic location. It should be noted that in studies that measure the prevalence of exploitation in locations, there is not necessarily a direct correlation between the number of locations used for exploitation and the number of people who are victimized there or the number of people committing the abuse. With IP addresses, in particular, a single person may use multiple IP addresses while engaging in OSEC and a single IP address may be used by multiple people who are engaging in OSEC. Similarly, a single IP address can be associated with multiple geographic locations (e.g., if multiple homes share a router or if an ISP is using network address translation [NAT][81]). Therefore, the relationship between number of IP addresses associated with OSEC activity, the number of geographic locations where OSEC occurs, and the number of OSEC victims or traffickers is unknown.

Mark-recapture methodology refers to a class of estimation procedures that originated in the environmental sciences to quantify wildlife populations. In recent decades, however, the method has become a popular choice for estimating the population of hard-to-reach human populations (e.g., people who are homeless,[82,83,84] use drugs,[85,86] or are living with HIV[87]) that are often

[80] See Appendix B for a description of other methodologies considered, including methodologies that directly measure human populations, and the challenges associated with them.

[81] NAT is when one public IP address is used to route information to/from multiple private IP addresses.

[82] Williams. (2010). Can we measure homelessness? A critical evaluation of 'Capture-Recapture'. *Methodological Innovations Online*, 5(2), 49-59.

[83] Stark, et al. (2017). Estimating the size of the homeless adolescent population across seven cities in Cambodia. *BMC Medical Research Methodology,* 17(13).

[84] Schepers & Nicaise. (2017). *Working Paper: Estimating the Homeless Population, Sampling Strategies*. HIV A Research Institute for Work and Society: Leuven, Belgium.

[85] Gemmell, Millar, & Hay. (2004). Capture-recapture estimates of problem drug use and the use of simulation-based confidence intervals in a stratified analysis. *Journal of Epidemiology and Community Health,* 58, 758-765.

[86] Xu, Fyfe, Walker, & Crown. (2014). Estimating the number of injection drug users in Greater Victoria, Canada using capture-recapture methods. *Harm Reduction Journal*, 11(9).

[87] Poorolajal, Mohammadi, & Farzinara. (2017). Using the capture-recapture method to estimate the human immunodeficiency virus-positive population. *Epidemiology and Health,* 39.

missed through traditional sampling techniques. The concept behind the method is that by quantifying the overlap between two or more "captures" (samples) of the population of interest, one can estimate the total size of the population of interest. When using mark-recapture methodology to estimate human populations, "capture occasions" are typically surveys. However, a variant of the method, called multiple systems estimation (MSE), uses administrative lists to collect retrospective "captures."

MSE is a generalization of mark-recapture procedures, tailored to address common issues found in administrative lists. Oftentimes, such lists are based on law enforcement, hospitalization, and/or non-governmental records. Some recent and well-known applications include analyses of a data set of victims of modern slavery in the United Kingdom,[88] and a data set of human trafficking victims in The Netherlands.[89] This study was similar to MSE studies in that mark-recapture procedures were applied to secondary data sets to estimate the size of a hidden population. Therefore, this study may be considered a variation of MSE.

NCMEC's CyberTipline is the centralized mechanism where US-based ESPs report incidents of internet-based CSE. US law mandates that US-based ESPs report incidents of apparent child pornography of which they are aware on their platforms. The law also permits ESPs to report other instances of CSE. The general public can also make reports on the CyberTipline, but the majority of reports come from ESPs. Because many US-based ESPs have a global user base, NCMEC receives millions of CyberTipline reports each year related to internet-based CSE across the globe. CyberTipline reports geographically resolving to IP addresses from countries outside the US may be automatically forwarded to the appointed law enforcement agencies within those countries. Thus, it was possible to create a list of all CyberTipline reports resolving to IP addresses in the Philippines for the study period, 2010-2017.

For this study, the research team planned to split the list of CyberTipline reports resolving to IP addresses in the Philippines into multiple "captures" based on the time period in which the CyberTipline report was received by NCMEC. The overlap between the capture occasions, which are based on sets of data observed within time periods, could then be analyzed to estimate the total number of Philippine IP addresses associated with CSE. This number could then be divided by the total number of IP addresses assigned to the Philippines to get the percent of Philippine IP addresses used for CSE.

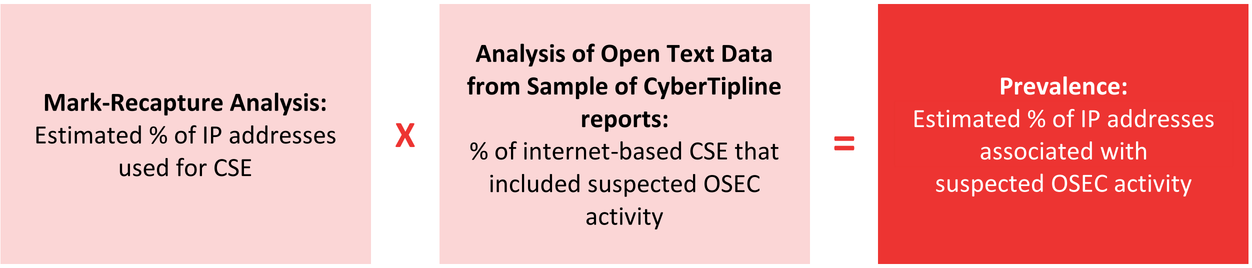
It should be noted, however, that internet-based CSE includes many crimes that are outside the study definition of OSEC. These include crimes like sharing CSEM (without financial compensation), grooming children for sexual exploitation, or arranging for in-person child sexual abuse.

Therefore, because OSEC, and not general internet-based CSE, was the ultimate subject of interest, the study team planned to conduct a more thorough review of a sample of CyberTipline reports to determine what percent of all CyberTipline reports in the Philippines included suspected OSEC activity. By extrapolating this percentage onto the estimated percent of Philippines IP addresses used for CSE (from the mark-recapture analysis), the study team planned to establish an estimate of the percent of Philippines IP addresses associated with suspected OSEC activity (See Figure 2). This final estimate would serve as an estimate of OSEC prevalence in the Philippines.

[88] Bales, K., Hesketh, O., and Silverman, B. W. (2015). Modern slavery in the UK: How many victims? *Significance* 12, 16-21.

[89] Cruyff, M., van Dijk, J., and van der Heijden, P. G. M. (2017). The challenge of counting victims of human trafficking: Not on the record: A multiple systems estimation of the numbers of human trafficking victims in the Netherlands in 2010-2015 by year, age, gender, and type of exploitation. *CHANCE* 30, 41-49.

FIGURE 2. Formula for Estimating the Percent of IP Addresses Associated with Suspected OSEC Activity



Mark-Recapture Analysis:
Estimated % of IP addresses used for CSE

X

Analysis of Open Text Data from Sample of CyberTipline reports:
% of internet-based CSE that included suspected OSEC activity

=

Prevalence:
Estimated % of IP addresses associated with suspected OSEC activity

Methods for the Mark-Recapture Analysis

The methods used for the mark-recapture portion of the prevalence study are summarized below.

Data Set Up

NCMEC provided the study team with a data set of all CyberTipline reports in which Philippine-based IP addresses were identified from the years 2010-2017. The data set excluded CyberTipline reports reporting viral/meme images.[90] The data set included 16 variables. (See Appendix A for a full list and description of the variables.) After the data set had been cleaned, it included a total of 193,405 entries of Philippine-based IP addresses identified in CyberTipline reports from 2010-2017.

No Philippine IP addresses were reported prior to late 2011, and very few were reported from 2011-2013. Because low levels of reporting create unreliable mark-recapture estimates, IP addresses reported prior to 2014 were removed from the analyses, leaving 183,184 entries in the data set, and estimates were created only for the years 2014-2017.

Statistical Models

Because the behavior of human populations can be drastically different from the wildlife populations that the mark-recapture methodology was initially designed to study, statisticians have developed a variety of advanced models to adjust the method for applications to human populations. Since this is the first attempt (to the researchers' knowledge) to use a mark-recapture methodology to estimate the prevalence of OSEC, it was unclear which statistical models would produce the best results. Therefore, various statistical mark-recapture extrapolation models using different estimators, capture periods, and numbers of captures were tested, and the results compared across models. For simplicity, only the best-fitting models are presented in this report. These include: (1) the "monthly"[91] estimates are based on the model using four captures of one-week each and the M_{th} model (based on time and heterogeneity effects) with Chao's lower bound estimator; and (2) the annual estimates are based on the model using 13 captures of four-weeks each and the open population estimator.

[90] Note: "Viral" images are files that circulate rapidly from one user to another. "Meme" images are files being shared/posted out of mimicry or other seemingly non-malicious intent. Researchers chose to exclude CyberTipline reports reporting viral/meme images because these rarely constitute OSEC, as defined by the study. However, NCMEC was only able to exclude reports that were labeled as viral/meme images by the ESP who submitted the CyberTipline report to NCMEC. Many CyberTipline reports relate to viral/meme images but are not labeled as such by the reporter. Because researchers had no way to identify CyberTipline reports related to viral/meme images that were not labeled as such by the reporter, without manually reviewing each report, those CyberTipline reports were included in the final data set.

[91] "Monthly" is a term used for simplicity of discussion. However, it relates to a four-week time period, not a calendar month.

Methods for the Collection and Analysis of Open Text Data within CyberTipline Reports

To estimate the percent of internet-based CSE that is associated with suspected OSEC activity, IJM criminal analysts reviewed the data within the open-ended text fields of a random sample of CyberTipline reports from 2015 and 2017. The 2015 sample included 966 unique CyberTipline reports related to 744 unique IP addresses, and the final 2017 sample included 1,289 unique CyberTipline reports related to 760 unique IP addresses.

To classify the CyberTipline reports, the criminal analysts used a data collection tool, which included six questions to guide them in determining if each CyberTipline report being reviewed was associated with suspected OSEC activity. Based on the answers to these questions, each CyberTipline report was classified as one of the following: “Not OSEC,” “Unlikely OSEC,” “Possible OSEC,” “OSEC,” or “Unknown.”

The data collection tool also included an open-ended text field for the analysts to write notes about the CyberTip, and these notes provided an interesting source of qualitative data. Researchers coded the data in these notes to pull out some anecdotal findings from this data collection effort. However, because these notes were not mandatory within the data collection tool, the criminal analysts did not consistently enter them. Therefore, the findings from these notes are not generalizable to all CyberTipline reports.

Limitations

When designing this study, researchers recognized multiple risks and potential limitations to the work. Some of these risks were realized in the implementation of the study, while others were found to have little impact on the quality of the study.

The first limitation affects the interpretation of the results. This methodology provides estimates of the number of IP addresses associated with suspected OSEC activity. It cannot serve as a proxy for the number of OSEC victims or traffickers in the Philippines. Although prevalence based on IP addresses is a less intuitive statistic than prevalence based on victims or traffickers, the study team decided that it was still useful enough to pursue. Therefore, this challenge was considered a concern to be managed when interpreting and disseminating results rather than a reason to reject the methodology.

The second limitation is related to the assumptions behind the methodology. Mark-recapture methodology requires two important assumptions (that the population is closed and that “marked”, and “unmarked” individuals have equal survival probabilities) to be true in order to provide meaningful results. It is unclear how well the design of this study conforms to those assumptions. Although advanced statistical models were used to adjust for potential assumption violations, there is still room to question the theoretical appropriateness of the model. Indeed model-fitting tests revealed that none of the models provided adequate fit. However, the results obtained between the various models and estimators were quite similar, which provides some assurance that the models are not too far off base.

The third limitation might affect the accuracy of the estimates. ESPs occasionally double report an event. Duplicate records can happen for a variety of reasons. For example, duplicate reports are created by some ESPs because they automatically send one image per report. Thus, if a user shares 50 images in a single chat session, 50 reports would be generated about that single event. This kind of duplicate report was not considered a problem, however, because the final data set for the mark-recapture analyses removed duplicate instances of IP addresses by day. Therefore, an IP address would only be re-counted if it was used for CSE on multiple days, which would correspond to multiple instances of CSE. Duplicate reports can also be created when ESPs use technology to scan user content and automatically report misuse when it is found. Misuse is simultaneously reported to NCMEC and sent to the ESP's records, where a human analyst can review it. If the analyst reviews it and finds additional case details that s/he wants to report to NCMEC, the analyst can fill out a manual form with that information. This would result in a double report of the event in NCMEC's system, which may come to NCMEC weeks or months after the initial event was reported. There was no way for the study team to identify and remove duplicate records from the mark-recapture analysis. However, this was not considered to be a significant problem because only 985 (<1%) of all entries in the data set were ESP Manual Forms (the only type of entry that *could* be a duplicate entry). Given that a vast amount of online child exploitation goes unidentified and unreported, the team does not believe the potential presence of a small number of duplicate entries has led to significant overestimates of the number of IP addresses used for CSE.

The final, and most impactful, limitation is related to the quantity and quality of CyberTipline data submitted by ESPs in CyberTipline reports. Because NCMEC receives CyberTipline reports from a variety of sources, there can be significant differences in the amount, type, and quality of data provided from the different sources. The OSEC status of 80% of CyberTipline reports reviewed could not be determined because the amount and/or quality of data in the open-ended text fields were insufficient[92]. After pulling two full samples of CyberTipline reports, the team was still unable to get a large enough sample to create results that could be generalized with the desired level of confidence and margin of error. Therefore, while this study was able to report the estimated percent of IP addresses used for CSE, it could not make any inferences on the percent of those IP addresses associated with suspected OSEC activity.

ASSESSING THE NATURE OF OSEC

In addition to estimating the scope of OSEC in the Philippines, the study team wanted to better understand the nature of OSEC in the Philippines. Questions related to the nature of OSEC included:

- How are OSEC investigations initiated in the Philippines?
- What are the demographics of OSEC victims, customers, and traffickers?
- What are the relationships between victims, customers, and traffickers?
- What methods are used to communicate between victims, customers, and traffickers?
- What types of materials are exchanged in OSEC cases?
- How much money is paid to exchange these materials?

For this, IJM and Philippine law enforcement agencies collaborated to conduct an in-depth case file review of all cases of OSEC investigated by the agencies between 2010 and 2017. This section provides a summary of the methods used in the case file review. For a more detailed description of the methods, see Appendix A.

Sampling Strategy

The primary law enforcement agencies that investigate OSEC cases in the Philippines are the Philippine National Police Women and Children Protection Center (PNP WCPC) and the National Bureau of Investigation - Anti-Human Trafficking Division (NBI-AHTRAD). The study team aimed to review case files for 100% of the cases referred to and/or investigated by these two law enforcement agencies between January 2010 and December 2017.

[92] It should be noted that NCMEC's purpose in providing the open-ended text fields is not necessarily to identify the type of conduct being reported. Many CyberTipline reporters use these fields to provide additional information related to the reported user or child victims. . Thus, poor data quality *for the purposes of this study* should not be considered to be poor data quality in general.

Definition and Description of Case Files

For this study, a "case" was defined as any one of the following:

- A case referred to Philippine law enforcement that had not yet been investigated by Philippine law enforcement;
- A case referred to Philippine law enforcement that had been investigated by Philippine law enforcement; or
- A case proactively generated and investigated by Philippine law enforcement without a referral.

Case referrals contained different types of information from Philippine investigation case files. Case referrals typically had more information on the customers and the criminal process used by the customers than on the Philippines-based traffickers or victims. Philippine investigation case files, on the other hand, typically contained little information on the customers but much more detailed information on the victims, traffickers, and the criminal process used by traffickers when interacting with undercover investigators.

For cases that had been referred to *and* investigated by Philippine law enforcement, the case referrals and the Philippine investigation case files were matched to create a single record, but the referral and investigation data were kept separate (e.g., data on the offending process found in the referral were recorded separately from data on the offending process found in the investigation case file). This allowed researchers to compare information found in both the case referral and the investigation case file to identify similarities and differences in (1) the number and characteristics of victims identified in case referrals vs. investigation case files, and (2) the criminal processes reported in case referrals (detailing interactions between real OSEC customers and traffickers) vs. investigation files (detailing interactions between undercover investigators and OSEC traffickers).

Data Collection

IJM's research, OSEC program, and law enforcement development teams collaborated to create the data collection tool. The final instrument had a total of 61 questions and took an average of 50 minutes to complete. The tool captured information on:

- How the case was initiated and if it had been investigated by Philippine law enforcement;
- The OSEC victims, customers, traffickers, and criminal processes recorded in the case referral (if one was received by Philippine law enforcement);
- The OSEC victims, customers, traffickers, and criminal processes recorded in the Philippine law enforcement investigation case file (if an investigation had led to an operation, arrest, or victim rescue).

A single enumerator recorded the data on all the case files in the study. However, an IJM OSEC investigator accompanied the enumerator on each case file review and navigated the case files to pull out the relevant information for the enumerator to record. This made the process more efficient and prevented the enumerator from seeing most of the highly sensitive data contained in the case files.

Data were collected from two primary sources: Philippine law enforcement case files and IJM case files. IJM has supported almost all OSEC investigations conducted by Philippine law enforcement. For program purposes, IJM keeps its own records of cases. To minimize the amount of time (and thus, disruption) spent collecting data at the Philippines law enforcement offices, enumerators first collected data on IJM-supported cases using IJM case files. They then moved to the offices of the Philippines law enforcement agencies that stored the law enforcement case files.

Researchers successfully collected data on all cases investigated by PNP WCPC or NBI-AHTRAD and on all cases referred to PNP WCPC. However, the team was not able to collect data on OSEC referrals to NBI-AHTRAD that had not led to an operation, rescue, or arrest. Thus, the final sample included 100% of OSEC cases referred to PNP WCPC, but only the cases referred to NBI-AHTRAD that had been investigated and resulted in an operation, arrest, or rescue. Table 1 presents the total number of cases reviewed, disaggregated by type of case file.[93]

TABLE 1. Case File Review Sample

	Total
Total Case Files Reviewed	**92**
Case Referral Only	21
PHI Investigation Only	28
Case Referral + PHI Investigation	43

Data Handling and Analysis

The enumerator collected case file data using a laptop and a secure online survey platform, eliminating the need for manual data entry. The online survey platform protected submitted data using AES-256 encryption.

A researcher quality-checked more than 15% of case files to ensure that all questions were answered and that answers followed logical patterns (e.g., if the data showed that four victims were identified in a case file, then the enumerator should have entered demographic data for four victims). All missing data and inconsistent patterns were immediately shared with the enumerator, and he was asked to provide an explanation for the inconsistencies or re-review the case file to find the missing data.

After all data were collected, researchers downloaded the final database onto their password-protected laptops for cleaning and analysis. Data cleaning, recoding, and data analysis were conducted using Excel.

Limitations

Two primary limitations were identified in this study. First, the team was not able to collect data on any OSEC cases referred to NBI-AHTRAD that had not resulted in an operation, arrest, or rescue. Nor was the team able to determine how many such cases existed. OSEC cases at NBI-AHTRAD are not labeled as “OSEC” cases but are given the broader label of “Trafficking” cases. Case data are not stored in a database, and case files are not stored in a single location but are

[93] Note: There is a discrepancy between the number of cases referred to the Philippines as reported by international law enforcement data and Philippine law enforcement case data. Possible explanations for these discrepancies include: (1) For this study, researchers only looked at cases reported to PNP and NBI—the law enforcement agencies within the Philippines that most often investigate OSEC cases. However, international law enforcement agencies may have referred cases to other Philippine law enforcement agencies, and the cases may not have been transferred to PNP or NBI. (2) Philippine law enforcement may label cases differently than international law enforcement does. For example, if multiple international case referrals pointed to the same Philippine trafficker, Philippine law enforcement may have combined the referrals into a single case file. (3) Each international law enforcement agency uses a slightly different definition of OSEC. It may be that some cases labeled as “OSEC” by international law enforcement agencies were labeled as a different crime by Philippine law enforcement and thus were not counted in their case files.

distributed to the investigator in charge of each case. Therefore, there was no way for researchers to sort through “Trafficking” case files to identify and review the OSEC cases, without significantly disrupting the NBI-AHTRAD investigators’ work. Therefore, the final sample included 100% of PNP WCPC’s OSEC case files (investigations and referrals) and a nonrandom sample of an unknown percent of NBI-AHTRAD’s OSEC case files (investigations only). This may limit the generalizability of the results. However, based on their experience, IJM’s OSEC and law enforcement development teams had no reason to believe that the missing cases represent a particularly large proportion of all cases, or that the non-investigated NBI-AHTRAD OSEC cases differ significantly from investigated NBI-AHTRAD OSEC cases. Thus, the study team does not think that the inability to collect this data significantly undermines the representativeness of the results.

Second, while the researchers believe that the results of this portion of the study are representative of OSEC cases that have been referred to or investigated by Philippine anti-trafficking units, it is not necessarily representative of all *incidents* of OSEC. There may be some characteristics of the studied cases (including characteristics of the victims, customers, traffickers, or criminal processes) that make them more likely to be investigated than other incidents of OSEC. For example, some countries’ law enforcement agencies are more proactive and efficient at, and/or have more resources allocated to, investigating OSEC customers in their own countries and sharing relevant evidence with Philippine law enforcement. Naturally, the study showed that most customers are from these countries, even though there may be many customers from other countries that put fewer resources into investigating these crimes and who thus remain uncaught. Therefore, this research is skewed towards the processes and people that are more likely to be detected. Similarly, for the study period (2010-2017), Philippine law enforcement did not have equal capacity to investigate OSEC cases in all areas of the country, so the geographic distribution of cases was as much a function of law enforcement capacity as actual OSEC incidence.

EXAMINING THE PHILIPPINES AS A GLOBAL HOTSPOT FOR OSEC

Among law enforcement experts and other practitioners engaged in responding to OSEC, the Philippines is often acknowledged as a global hotspot for OSEC. However, little data has been published to support this idea which, to date, has largely been based on the professional experience of law enforcement. Therefore, as part of this study, the research team collated all data they could access to compare the scope of OSEC in the Philippines to other potential source countries (i.e., countries in which OSEC victims or their traffickers are found) globally. This section describes the data collected for this effort. Because data on global incidents of OSEC are limited and fragmented across multiple sources, the study team conducted two separate data collection and analysis efforts to explore this research objective.

Global Law Enforcement Data Collection and Analysis

The study team solicited data from twelve VGT agencies[94] regarding the number of OSEC cases each agency had investigated. The team specifically asked for data on cases that (1) had been investigated between 2010 and 2017, and (2) had been referred to a different country’s law enforcement because they involved traffickers or victims from that country. Four of the twelve agencies were able to share this data with us for public use: the Royal Canadian Mounted Police (RCMP), the United Kingdom National Crime Agency (NCA), the United States Federal Bureau

[94] For a list of VGT members, see virtualglobaltaskforce.com

of Investigation (FBI), and the Nordic Liaison Office (NLO) representing Norway, Sweden, Denmark, Finland and Iceland. These data were aggregated to determine the total number of cases involving each identified source country over the eight-year period.

Limitations

There are three major limitations to this data. First, data are based on a convenience sample of law enforcement agencies—those that had the ability to share data with the study team. Cases coming from these four agencies were not necessarily representative of cases coming from other law enforcement agencies, much less of incidents of OSEC that went undetected. There may have been countries with few or no OSEC referrals that actually had a large number of OSEC incidents during the study period.

Second, in some countries, multiple law enforcement agencies within a country can refer international OSEC cases to other countries. The data submitted by law enforcement agencies in those countries represented only a portion of all OSEC referrals coming from their country. For example, in the US, there are multiple law enforcement agencies that investigate OSEC cases—not just the FBI. If an investigation leads to evidence of victims or traffickers in another country, any US law enforcement agency investigating the case can share that information with the related country's law enforcement. Therefore, the number of OSEC cases the FBI referred to another country is less than the total number of cases all US law enforcement agencies referred to another country. Thus, the data presented in this report should not be viewed as representative of all OSEC cases emerging from these countries.

Finally, each law enforcement agency defines OSEC a little differently, so the results presented are not necessarily representative of OSEC *as it is defined in this study*. Overall, these results should be interpreted only as exploratory data on the global scope of OSEC based on the data that was available at this level from across law enforcement agencies.

NCMEC Online Enticement Data

Researchers also solicited another data set (separate from the one used for prevalence estimation) from NCMEC. As mentioned previously, NCMEC's CyberTipline is the centralized mechanism for reporting the internet-based child sexual exploitation in the US. Because many US-based ESPs have a global user base (e.g., Facebook, Google, Microsoft), NCMEC receives CyberTipline reports related to countries around the world. Because of the volume of CyberTipline reports NCMEC receives, NCMEC analysts focus the majority of their time on reviewing CyberTipline reports that either have a US connection or are classified as high priority. Thus, a relatively small portion of all NCMEC analyst-reviewed CyberTipline reports involve countries outside the US.[95] This component of the study examines data available on NCMEC analyst-reviewed CyberTipline reports. These reports include information about the types of incidents being reported, as determined by NCMEC analysts.

Based on conversations with NCMEC staff, the study team determined that, if CyberTipline reports were reviewed by a NCMEC analyst, CyberTipline reports reporting incidents of OSEC, as defined by this study, would most likely be categorized as the incident type "online enticement of children." Based on the case file review and IJM's casework experience to date, the study team also knew that OSEC cases in the Philippines almost always involved international (non-Philippine-based) customers, and they hypothesized that this would be the

[95] Note: When NCMEC receives CyberTipline reports that relate to activity occurring outside of the US, NCMEC makes the CyberTipline report available to the relevant law enforcement agency within those countries when a direct connection to law enforcement is available. For reports resolving to countries without a direct law enforcement connection, elements of the CyberTipline reports are made available to Interpol. While these CyberTipline reports may not reviewed by NCMEC, they may still be acted upon by law enforcement.

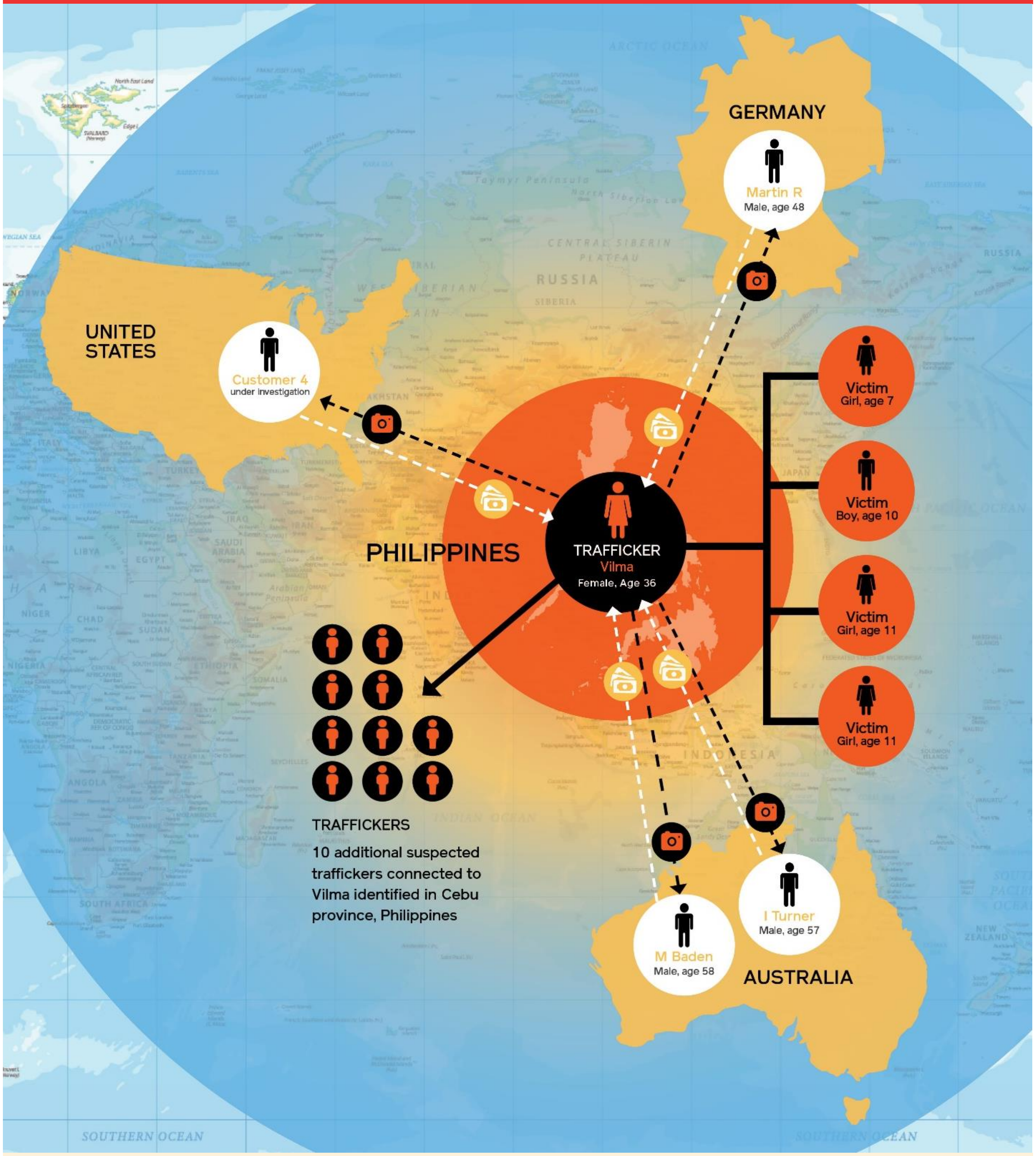
case for most source countries. Therefore, researchers requested that NCMEC send them the number of CyberTipline reports indicated as "online enticement" in the incident type category, which had been made available to law enforcement agencies in more than one country between 2010 and 2017. These data were disaggregated by the regions to which the CyberTipline reports had been sent.

Limitations

There are two major limitations to this data. First, because NCMEC focuses its efforts on reviewing US-based CyberTipline reports, most internationally based CyberTipline reports are forwarded automatically (auto-referred) to the relevant country's law enforcement without being reviewed. Thus, the CyberTipline reports in this sample represent a small, non-generalizable sample of all NCMEC CyberTipline reports related to "online enticement." There are two major limitations to this data. First, because NCMEC focuses its efforts on reviewing US-based CyberTipline reports, most internationally based CyberTipline reports are forwarded automatically (auto-referred) to the relevant country's law enforcement without being reviewed. Thus, the CyberTipline reports in this sample represent a small, non-generalizable sample of all NCMEC CyberTipline reports related to "online enticement."

Second, "online enticement" is only a rough proxy for OSEC, as defined by this study. CyberTipline reports categorized as "online enticement" include crimes that would not be defined as OSEC. For example, cases of child grooming, with no exchange of commercial compensation, would also be classified in the CyberTipline reports as "online enticement." Furthermore, many cases of OSEC could be labeled as something different than "online enticement." For example, if after engaging in OSEC, a customer asked to engage in contact abuse with the child, NCMEC analysts would likely categorize that report as "child sex tourism, pre-travel" rather than "online enticement."

SPOTLIGHT A Crime with Global Impact: People of the Philippines vs Vilma,[96] 2016



OSEC is a global crime, in which a single OSEC trafficker often engages with multiple OSEC customers from around the world, and in which a single OSEC customer often solicits abuse material from multiple OSEC traffickers. This global reach can serve to complicate the law

[96] Vilma is a pseudonym used in the Philippine press and for external publication in order to protect the victims that are related to the accused.

enforcement response. However, with strong global coordination among law enforcement agencies, a case starting with the investigation of a single perpetrator can cause a chain reaction, resulting in the arrest of multiple OSEC customers and traffickers and the rescue of many victims across the globe.

An emblematic example of this is the case of People of the Philippines vs. Vilma, 2016.

In 2016, Queensland Police Taskforce Argos arrested Australian national, I. Turner. Their investigation of Turner found that he was purchasing CSEM, including live-stream videos, originating from the Philippines. One of his Philippine suppliers was found to be Vilma. Thus, the Australian Federal Police (AFP) referred this case to Philippine National Police (PNP) shortly after Turner's arrest.

The PNP then conducted their own surveillance of Vilma. The investigation revealed that she was providing CSEM of her own children, in the form of recorded videos and pictures and live-streamed abuse to online offenders from the US, Australia and Germany. This material involved contact abuse directed by Vilma as she communicated with the overseas customers in real-time. Vilma communicated with her customers around the world through popular video-enabled social media platforms and email and charged varying fees for CSEM photos and livestreamed abuse.

Through, the investigation, it was discovered that the children had been abused and exploited over the span of 5-6 years. One daughter later remarked in an affidavit that she had been abused in so many live-stream videos that she had lost count. At the time of rescue, the children were aged 7 to 11.

On September 8, 2016, the PNP implemented a search warrant and arrest at Vilma's residence. That day, the four minor victims – Vilma's own children – were rescued. The children were then placed in the care and custody of the Philippine Department of Social Welfare and Development (DSWD) where they received therapy, counselling, psycho-social and other rehabilitation services. They are now living with a kinship foster parent, availing of government-sponsored kinship support which includes financial support for education and other development.

Vilma was charged with 1 count of qualified trafficking in persons, which carries a life sentence, along with attendant fines and damages. Although Vilma initially pled not guilty, she had a change of heart after Prosecution presented strong evidence, and the case ended early through a plea agreement. On June 6, 2018, Vilma entered a plea of guilty to the offence of simple trafficking in persons and was sentenced to 20 years imprisonment and ordered to pay a fine of PHP 1,000,000 (approx. 20,000 USD) as well as PHP 100,000 (approx. 2,000 USD) in moral damages and PHP 100,000 in exemplary damages to each of her victims.

Following Vilma's arrest, evidence collected by Philippine law enforcement helped to identify additional OSEC customers abroad and additional OSEC traffickers within the Philippines. Information on the customers was referred to the relevant countries' law enforcement agencies for follow-up. Investigations associated with Vilma's case resulted in the arrest and conviction of Martin R. in Germany for associated offenses in 2018, sentenced to four years and six months imprisonment; M. Baden in Australia for related charges in 2019, sentenced to seven years and four months imprisonment; and the conviction of I. Turner in Australia, sentenced to four years and six months in prison and eligible for parole after two years. Investigation of additional OSEC customers is still underway.

This case underscores the global nature of the OSEC crime: how, through the use of technology and the internet, perpetrators from all around the world can sexually abuse and exploit children. However, this case also highlights the ability of law enforcement to investigate networks of OSEC traffickers and customers around the world. With effective referral mechanisms and law enforcement coordination, abusers, whether traffickers or customers, can be brought to justice and their victims rescued from ongoing exploitation.

Results

ESTIMATING THE BASELINE PREVALENCE OF INTERNET-BASED CSE AND OSEC IN THE PHILIPPINES

This section presents the results of the analysis of the NCMEC CyberTipline reports resolving to IP addresses in the Philippines for the study period, 2010-2017. The first sub-section presents results of the analysis of the raw NCMEC CyberTipline data. The second and third sub-sections present the results of the mark-recapture analyses, which provide an estimate of the total number of IP addresses used for CSE, beyond those reported to NCMEC. The fourth sub-section presents the results of the in-depth analysis of open-text data within the CyberTipline reports.

KEY FINDINGS

1. There was a consistent, sharp rise in the number of IP addresses linked to the Philippines between 2014 and 2017.
2. The estimated number/prevalence rate of IP addresses used for CSE each month grew more than 12-fold between 2014 and 2017.
3. The estimated number/prevalence rate of IP addresses used for CSE each year more than doubled between 2014 and 2017.
4. Due to inconsistencies in the quality of the data within the open-ended text fields in CyberTipline report, it was not possible to estimate the percent of internet-based CSE that included suspected OSEC activity.

Characteristics of CyberTipline Reports

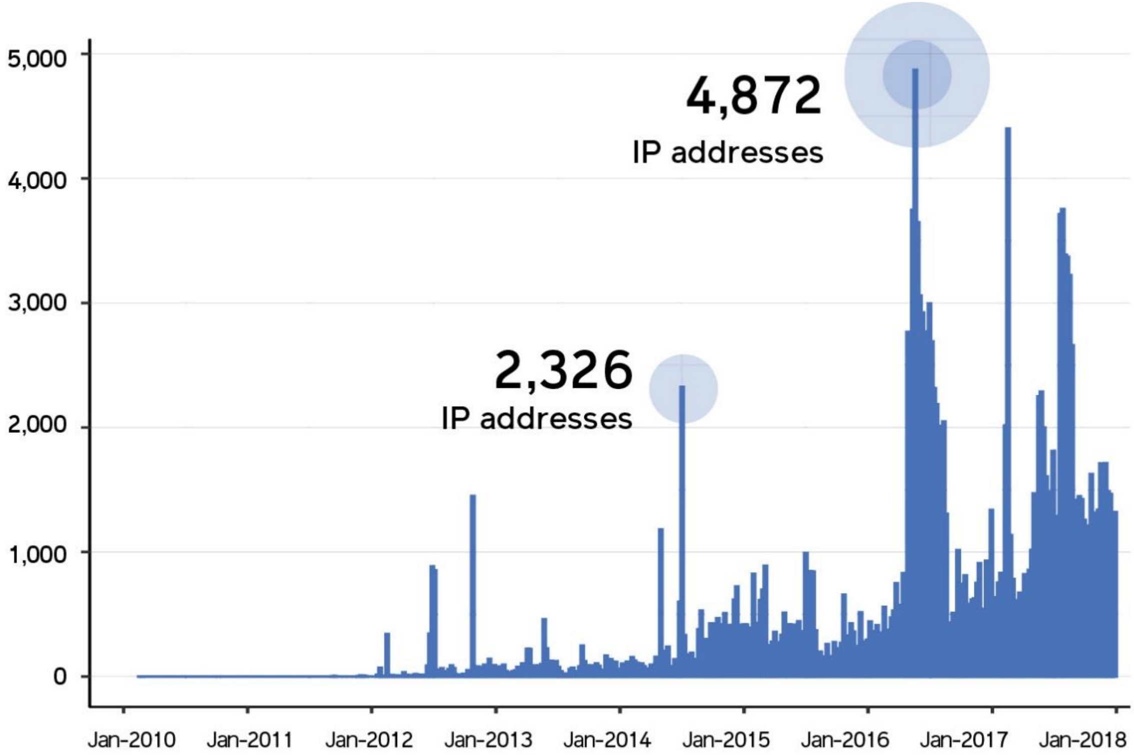
KEY FINDING #1

There was a consistent, sharp rise in the number of IP addresses linked to the Philippines between 2014 and 2017.

During the study period (2010-2017), a total of 125,032 Philippine-based CyberTipline reports matching the study criteria were reported to NCMEC. These CyberTipline reports identified 193,405 IP addresses resolving to the Philippines, 62% (119,179) of which were unique IP addresses (i.e., only reported one time) and 38% (74,226) of which were duplicates (i.e., IP addresses that were associated with more than one CyberTipline report). Figure 3 shows the distribution of the number of IP addresses reported to the Philippines each week from 2010-2017. Fewer than 10 Philippine IP addresses were reported prior to late 2011. Between 2011 and 2014, there were small spikes of activity,[97] but reporting remained low. Since 2014, however, there has been a consistent increase in the number of Philippine IP addresses reported to NCMEC in CyberTipline reports.

[97] During this time period, most ESPs submitted CyberTipline reports in batches. The study team expects that the spikes of activity are caused by batch submissions, rather than seasonal trends in perpetration of online crime.

FIGURE 3. Number of IP Addresses Reported to the Philippines Weekly, 2010-2017



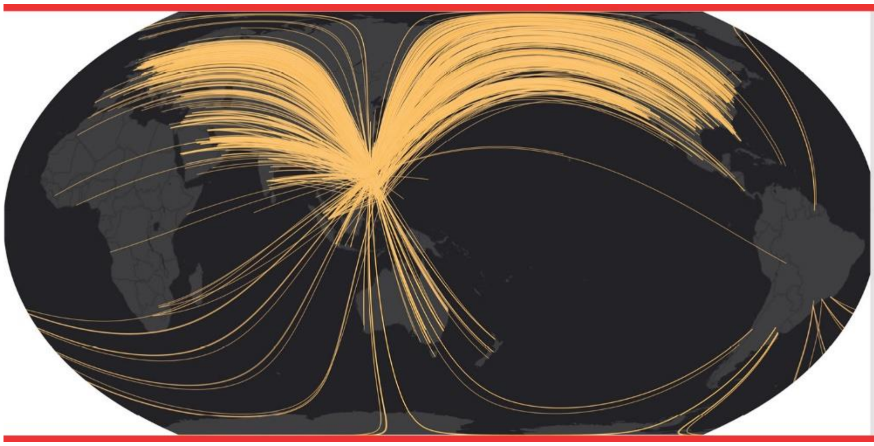
Of all IP addresses reported, more than 99% (192,882) were associated with CyberTipline reports that had been automatically submitted to NCMEC from ESPs, and less than 1% (514) were associated with CyberTipline reports that had been manually submitted by ESPs. In other words, the vast majority of conduct reported to NCMEC was originally detected by digital algorithms created by ESPs to identify illegal activity on their platforms and were not reviewed by ESP analysts prior to being submitted to NCMEC.

After being received by NCMEC, most CyberTipline reports associated with non-US IP addresses are auto-referred to the relevant country's law enforcement without further review. In this study, over 99% of IP addresses (191,929) were associated with CyberTipline reports that had been auto-referred to the Philippines without review by a NCMEC analyst. Of the 1,476 that did receive NCMEC review, 79% (1,167) were categorized by NCMEC as "apparent child pornography," and another 11% (156) were categorized as "online enticement pre-travel." NCMEC analysts confirmed that incidents of what this study defines as OSEC could be categorized into any of those groups (auto-referred without review, apparent child pornography, or online enticement pre-travel).

Less than 1% of IP addresses (560) were associated with CyberTipline reports containing possible new child sexual abuse material (CSAM). Only eight IP addresses were reported as possibly using a proxy IP address.

For more details on the characteristics of the raw NCMEC CyberTipline data, including the number of IP addresses captured in each four-week period, see Appendix C.

FIGURE 4. Links Between IP Addresses in the Philippines and Other Countries



This map was created by IP addresses included in NCMEC CyberTipline reports to the Philippines, between 2014 and 2017. Lines show links between IP addresses in the Philippines and IP addresses identified in other countries by CyberTip ID.

Monthly Prevalence Estimates of IP Addresses Used for CSE

KEY FINDING #2

The estimated number/prevalence rate of IP addresses used for CSE each month grew more than 12-fold between 2014 and 2017.

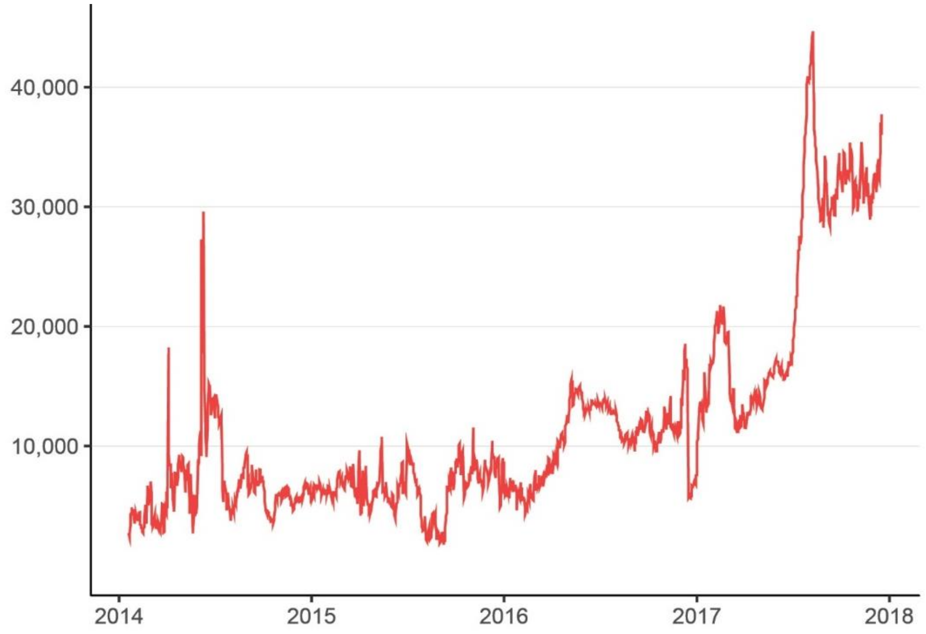
Based on the mark-recapture analysis, an estimated 2,723 (95% confidence interval [CI]: 1,516-3,930) IP addresses were used for CSE in the first four weeks of 2014. (Note: Mark-recapture estimates include IP addresses reported to NCMEC plus an estimate of those *not* reported.) By the last four weeks of 2017, the estimated number of IP addresses used for CSE grew to 37,735 (95% CI: 33,318-42,151).

The total number of IPv4 addresses[98] assigned to the Philippines (about 5.485 million) has remained relatively steady since 2011.[99,100] Thus, the growth in prevalence rate of IP addresses used for CSE is proportional to the growth in number of IP addresses used for CSE. In the first four weeks of 2014, about five in every 10,000 IP addresses were used for CSE. But by the last four weeks in 2017, an estimated 69 in every 10,000 IP addresses were used for CSE.

Figure 5 shows how the estimated number of IP addresses used for CSE changed from 2014 to 2017. Each point on the line represents the estimated number of IP addresses used for CSE in the four-week period prior to that day. This figure shows that with the exception of a short but notable spike in mid-2014, the estimated number of IP addresses used for CSE wavered between 3,000-10,000 per month in 2014 and 2015. Between the beginning of 2016 and the end of 2017, however, the estimated number of IP addresses used for CSE roughly quadrupled, growing from less than 10,000 per month in early 2016 to more than 40,000 per month at some periods of 2017. (See Appendix D for a table of the estimated number of IP addresses used for CSE in each four-week time period between 2014 and 2017.)

[98] Note: To calculate prevalence rates, the study team decided to use the number of IPv4 addresses, excluding newer IPv6 addresses. The reasons for this are two-fold. First, visible IPv6 addresses make up a small percentage of the entire market in the Philippines. As of 2018, fewer than 70,000 IPv6 addresses in the Philippines were visible. Second, very few IPv6 addresses (144) were identified in the NCMEC data set. Thus, it seemed simpler to remove IPv6 addresses from the data set and calculate prevalence only for IPv4 addresses.
[99] Mulingbayan, A. (2018.) APNIC Update for the Philippines. Retrieved from https://www.slideshare.net/apnic/phnog-2018-apnic-update
[100] Dalal, M. (2019.) IPv6: Powering the Next-generation Internet. Retrieved from http://philv6forum.org/blog/ipv6-powering-the-next-generation-internet/

FIGURE 5. Estimated Number of IP Addresses Used for CSE in Each Four-Week Time Period between 2014 and 2017



Annual Prevalence Estimates of IP Addresses Used for CSE

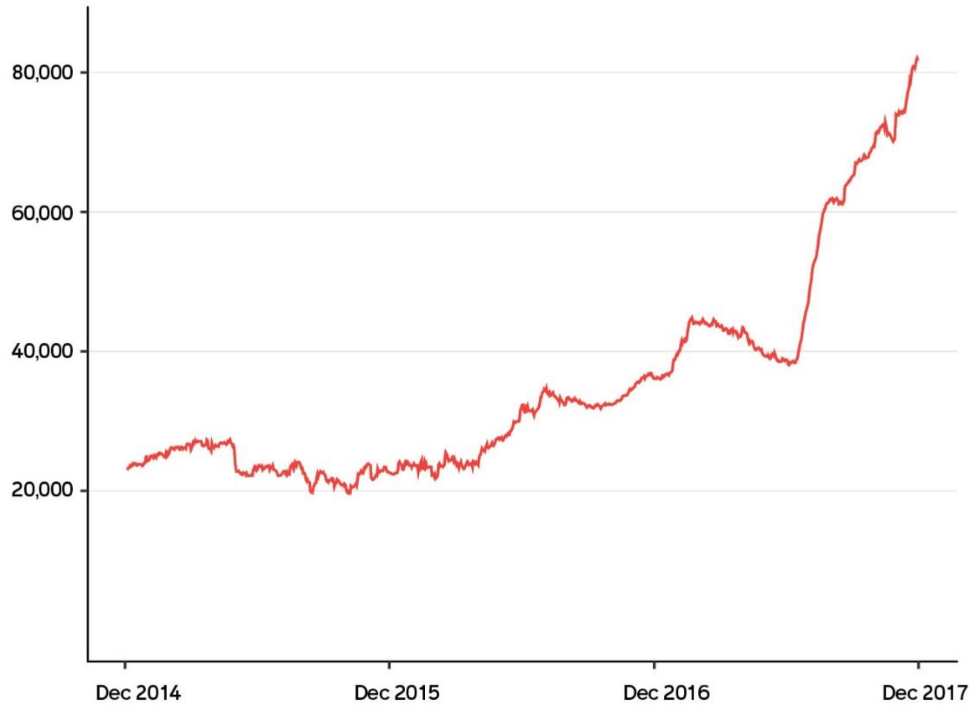
KEY FINDING #3

The estimated number/prevalence rate of IP addresses used for CSE each year more than tripled between 2014 and 2017.

Based on the mark-recapture analysis, the estimated number of IP addresses used for CSE has risen from around 23,333 (95% CI: 22,314-24,352) in 2014 to 81,723 (95% CI: 80,188-83,259) in 2017. This corresponds to a growth in the prevalence rate from about 43 out of every 10,000 IP addresses being used for CSE in 2014 to 149 out of every 10,000 IP addresses being used for CSE in 2017.

Figure 6 is similar to Figure 5 except that each point on the line represents the estimated number of IP addresses used for CSE in the *year* (365 days) prior to that point. The point on the line above the 2015 tick mark represents the estimated number of IP addresses used for CSE in 2014, and the point on the line above the 2017 tick mark represents the number of IP addresses used for CSE in 2017. Like the monthly estimates, the yearly estimates show a relatively steady number of IP addresses used for CSE in 2014 and 2015, with a sharp increase in the number of IP addresses used for CSE occurring between 2016 and 2017. (See Appendix D for a table of the estimated number of IP addresses used for CSE in each 365-day time period between 2014 and 2017.)

FIGURE 6. Estimated Number of IP Addresses Used for CSE in Each 365-Day Time Period between 2014 and 2017



The Percent of All Internet-Based CSE that is OSEC

KEY FINDING #4

Due to inconsistencies in the quality of the data within the open-ended text fields in CyberTipline reports, it was not possible to estimate the percent of internet-based CSE that included suspected OSEC activity.

As discussed in the Methodology, the study team tried to determine the percent of all CyberTipline reports that were associated with suspected OSEC activity by reviewing a random sample of 2,255 CyberTipline reports that contained at least some open-ended text. However, due to inconsistencies in the quality of the data within the open-ended text fields, the team was not able to classify the vast majority (about 80%) of the 2,255 CyberTipline reports they reviewed. As a result, researchers were not able to gather enough data to accurately report on the percent of IP addresses that were associated with suspected OSEC activity. With the data that were collected, any analyses would have had low confidence levels and high margins of error. The team did not feel confident that the analyses would produce meaningful results, so this portion of the analysis was ultimately abandoned.

However, the team was able to analyze the anecdotal data collected in the criminal analysts' notes. Three interesting findings arose from that data. First, the criminal analysts' notes indicated that at least 731 CyberTipline reports contained chat logs. In about 71% (516) of the chat logs, the primary language used was Tagalog or Filipino (apart from certain sexual references which tended to be in English). Most of the chatlogs contained in these CyberTipline reports were too short for researchers to determine whether these CyberTipline reports were cases of OSEC vs. other types of internet based CSE. However, this suggests that there *may be* a population of domestic, or at least Filipino- or Tagalog-fluent, offenders engaged in some type of CSEM sharing that has been relatively unaddressed by law enforcement. IJM OSEC investigation experts theorize that these offenders are *not* engaged in OSEC, as it is defined in this study, because any Philippine-based offender with enough money to purchase OSEC could also afford to engage in contact abuse. Rather, this finding likely points to the great variety of types of internet-based CSE found in NCMEC CyberTipline reports and the importance of distinguishing OSEC prevalence from the prevalence of internet-based CSE.

Second, none of the CyberTipline reports reviewed involved the sharing of videos or livestreaming abuse, despite the fact that these are common practices among OSEC customers and traffickers.[101] A couple of CyberTipline reports included extended chat logs in which the users indicated their intent to switch platforms to begin a video chat, but the content of the video chat was not picked up in the report since it occurred on a different platform than the one reporting the incident.

Finally, about 18% (405) of the CyberTipline reports reviewed by the criminal analysts reported on viral images or memes, despite the fact that NCMEC had removed from the data set all CyberTipline reports labeled by the reporting ESP as containing viral/meme images. This highlights how variations in the way ESPs submit reports can impede research efforts. NCMEC CyberTipline reports include an optional question that ESPs can answer to indicate that the report contains viral/meme images. However, ESPs may choose to skip that question and instead inform NCMEC that the report contains viral/meme images in one of the open-text fields. Because the open-text fields cannot be automatically coded like the close-ended fields can, these CyberTipline reports do not get labeled as containing viral/meme images, and so the final data set included many mislabeled CyberTipline reports. The second and third anecdotal findings from the criminal analysts' notes point to the need for improved identification of internet-based CSE and more standardized methods of CyberTipline reporting by ESPs to improve the NCMEC data's value for research.

ASSESSING THE NATURE OF OSEC

This section presents the results of the in-depth review of PNP WCPC and NBI-AHTRAD OSEC case files between 2010-2017. A total of 92 case files were reviewed, including: 21 case referrals for cases that had been referred to PNP WCPC by international law enforcement agencies but not yet investigated by Philippine law enforcement; 28 investigation files for cases that had been investigated by Philippine law enforcement but had no corresponding international law enforcement agency case referral; and case referrals and investigation files for 43 cases that were both referred to Philippine law enforcement by international law enforcement agencies *and* investigated by Philippine law enforcement.

The case file review results are broken into five sub-sections. The first sub-section presents data about how Philippine OSEC cases were initiated. The second, third, and fourth sub-sections present data about the typologies of OSEC victims, customers, and traffickers, respectively. The fourth sub-section presents data on the offending process, such as the language and platforms used to communicate, the types of CSEM exchanged, and the amount of money exchanged.

Key Findings

[101] See results from the review of Philippine law enforcement case files, particularly the section on the offending process, in the next section of the report.

1. The majority (64%) of Philippine OSEC cases were initiated by referrals from international law enforcement agencies.
2. The annual number of cases referred to and/or investigated by Philippine anti-trafficking units increased sharply and consistently from 2014 (1 case) to 2017 (43 cases).
3. The characteristics of OSEC victims were distinct from those of victims of establishment-based sexual exploitation of children.
4. OSEC was usually a family-based crime.
5. Without intervention, the abuse usually lasted for years.
6. Customers tended to be older men.
7. Customers tended to be from Western countries, although many had traveled to or lived in the Philippines at some point in time.
8. There was an average of two traffickers per case.
9. Traffickers tended to be younger Filipina women, often family members of the victims.
10. Most criminals who got caught communicated in English.
11. The crime occurred on the surface of the internet.
12. There appears to be a financial motivation to the crime for most facilitators of OSEC.

OSEC Case Initiation

KEY FINDING #1

The majority (64%; 59 cases) of Philippine OSEC cases were initiated by referrals from international law enforcement agencies.

INTERNATIONAL LAW ENFORCEMENT

Most Philippine OSEC cases began with referrals from international law enforcement agencies. Another large portion of cases (22%; 20 cases) started with information provided by a non-governmental organization (mostly referrals from IJM). The remaining cases were initiated by information provided by private citizens (5%; 5 cases), the Philippine Department of Justice Office of Cybercrime (5%; 5 cases), proactive Philippine law enforcement investigative efforts (2%; 1 case), and other means (2%; 1 case).

Of cases initiated through international law enforcement referrals, most came from the United States (31 cases; 55%), Nordic Liaison Office[102] (NLO; 13 cases; 22%), and Australia (7 cases; 12%). Others came from the United Kingdom (7%; 4 cases), Canada (2%; 1 case), and New Zealand (2%; 1 case).

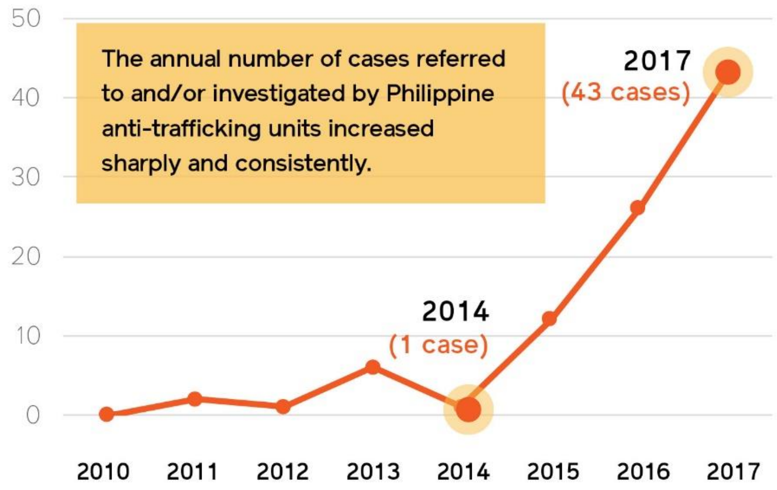
[102] The Nordic Liaison Office covers Denmark, Finland, Iceland, Norway and Sweden.

KEY FINDING #2

The annual number of cases referred to and/or investigated by Philippine anti-trafficking units increased sharply and consistently from 2014 (1 case) to 2017 (43 cases).

Although the total number of cases (92) was small for an eight-year time period, it represents a growing trend in the number of OSEC cases referred to and investigated by Philippine law enforcement. The majority of the growth occurred after 2014. (See Figure 7.) Between 2010 and 2014, only 10 OSEC cases were referred to or investigated by Philippine law enforcement—usually just one or two cases per year, with a small uptick of six cases in 2013. Between 2015 and 2017, the number of OSEC cases nearly doubled every year, ending with 43 cases referred or investigated in 2017. Of all cases referred to or initiated by Philippine anti-trafficking units during this time period, 77% (71 cases) had resulted in a rescue or arrest operation by the end of 2017.

FIGURE 7. Number of OSEC Cases Referred to and/or Investigated by Philippine Law Enforcement by Year, 2010-2017



OSEC Victim Typology

381 victims

Philippine and international law enforcement agencies identified 381 victims[103] in 90 OSEC cases[104] investigated between 2011 and 2017. That represents an average of more than four victims/case, with 10 cases involving 10 or more victims. Three key findings arose from the case file data about victims.

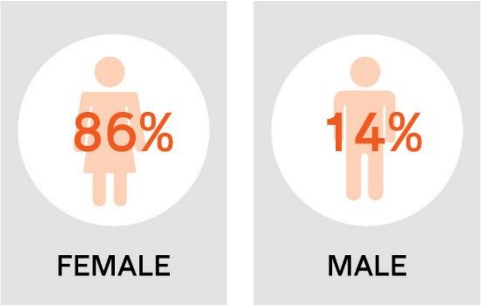
[103] The "total # of victims" includes all victims identified in the international law enforcement referral or the Philippines investigation. Where a victim identified in the Philippines investigation was known to be the same as a victim identified in the international law enforcement referral, this was counted as a single victim. Where there were discrepancies between referral and investigation data about the same victims (e.g., the referral reported the victim was 8 years old and the investigation reported the victim was 7 years old), investigation data were used in the analysis. This was because case referrals often contained estimates or best guesses for victim information, while investigations usually contained more accurate data.

[104] "Total number of cases" excludes two cases for which the total # of victims in the referral was "Unknown" and either there was no Philippines investigation completed or no victims were found during the Philippines investigation. One case had an unknown number of victims in the Philippines investigation but a known number of victims in the referral. 15 cases had an unknown # of victims in the referral but a known number of victims in the Philippines investigation. These 16 cases where the number of victims in either the referral or the Philippines investigation, but not both, were unknown were included in the analysis.

KEY FINDING #3

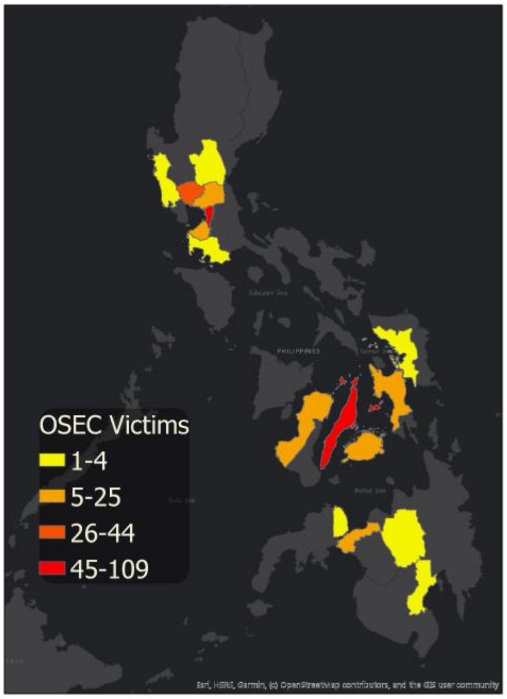
The characteristics of OSEC victims were distinct from those of child victims of street and establishment-based sexual exploitation (CSEC).

Philippine law enforcement agencies and non-profit organizations have been fighting street and establishment-based sexual exploitation of children for decades and have learned a great deal about the victims of these crimes. However, much less has been published on the victims of OSEC. In presenting the findings from the case file review, the study team decided to compare these findings with data on CSEC victims to highlight the different approaches needed when working with this population. Statistics on CSEC victims are based on the totality of IJM's casework supporting the Government of the Philippines in combatting CSEC from 2001 to 2016.



While victims of CSEC were almost all (96%) female, a significant number of OSEC victims (14%; 53 victims) were male. Victims of OSEC also tended to be much younger than CSEC victims. The average age of OSEC victims at the time of referral or rescue[105] was 11 years old, with ages ranging from less than one year old to 31 years old[106]. In comparison, the average age of CSEC victims at the time of rescue was 19 years old, with ages ranging from 4 to 35 years old[107]. Finally, whereas CSEC victims were often found in CSEC hot spots, OSEC victims were far more dispersed. As shown in Figure 8, OSEC victims have been found throughout the Philippines. The highest density of OSEC victims was found in the National Capitol Region (NCR). However, this is to be expected since the population of NCR is almost three times higher than the next most populated province in the Philippines.

FIGURE 8. Heat Map of OSEC Victim Locations



Esri, HERE, Garmin, (c) OpenStreetMap contributors, and the GIS user community

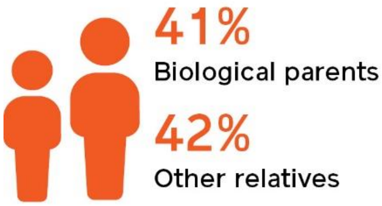
[105] Note: Because data on victims come from both case referrals and investigations, some ages are for victims at the time of referral and others for victims at the time of rescue.

[106] Note: Of the 381 victims identified in the OSEC case files, 41 were 18 years or above. Although these victims are not minors (as required by the study's definition of OSEC), they are still considered to be trafficking victims according to Philippine law and were thus included in the analyses. All but two adult victims were identified in cases that also involved minor victims. The two adult victims that were not identified in a case that also involved minor victims were identified together and were both 18 years old at the time of their rescue.

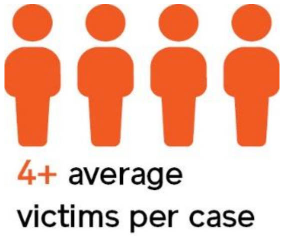
[107] Note: Although victims of OSEC and CSEC are, by definition, children, it is not uncommon to find adult victims of the same types of abuse when investigating these crimes against children. Law enforcement counts these as victims of OSEC even though they are not children. This study found that 6% of all OSEC victims were 18 years or above at the time of rescue or case referral. Comparatively, 62% of all CSEC victims identified through IJM's casework were 18 years or above at the time of rescue.

KEY FINDING #4

OSEC was usually a family-based crime.



Biological parents facilitated the abuse of 41% of all victims (89 victims), and other relatives facilitated the abuse of another 42% of victims (90 victims[108]). Furthermore, many children experienced OSEC victimization alongside other family members. Of the 285 victims that had been rescued, about 96% (275 victims) were rescued at the same time as at least one other person. Of these, 40% (110 victims) were siblings, and another 13% (36 victims) shared some other familial relationship (e.g., cousin). The relationship between victims rescued together was unknown for 39% of victims (106 victims).



KEY FINDING #5

Without intervention, the abuse often lasted for years.

Among the 43 victims for whom the exact length of abuse was known, the average length of abuse was two years, with length of abuse ranging from two months to four years. Just over 20% of these victims (9 victims) were abused for one year or less; 47% (20 victims) were abused for one to two years; and 33% (14 victims) were abused for three to four years. There did not seem to be any correlation between the age of the victim and the length of the abuse—children as young as six years old had been abused for four years, and victims as old as 20 years old[109] reported being abused for only 2 months. However, because length of abuse is primarily self-reported, we lack data on most children under the age of six years old. Further research is needed to better understand the victimology of OSEC survivors.

OSEC Customer Typology

OSEC customers are the offenders who drive demand for new sexual abuse and exploitation of children by instructing and paying in-person traffickers to exploit children. OSEC customers also produce CSEM when they direct sexual abuse remotely and when they entice, solicit, or coerce minors to produce sexually explicit videos and images for their personal consumption and distribution. Although they are offenders, they are referred to in this report as "customers" to easily distinguish them from traffickers and highlight the commercial nature of their crime.

Customers are not the primary focus of Philippine law enforcement OSEC investigations. Rather, Philippine law enforcement focuses on gathering evidence against in-country OSEC traffickers for the purposes of prosecution. Therefore, this study was limited in its ability to capture data on the offenders engaged as OSEC customers who have purchased CSEM from the Philippines. Of the 64 cases that were referred to Philippines law enforcement from another law

[108] These statistics were calculated for the 217 victims for whom the relationship between the victim and the trafficker was known.
[109] Note: Of the 381 victims identified in the OSEC case files, 41 were 18 years or above. Although these victims are not minors (as required by the study's definition of OSEC), they are still considered to be trafficking victims according to Philippine law and were thus included in the analyses. All but two adult victims were identified in cases that also involved minor victims. The two adult victims that were not identified in a case that also involved minor victims were identified together and were both 18 years old at the time of their rescue.

enforcement agency, only 44 cases had data about the international customers of the crime, and each of these cases does not necessarily represent a unique customer. For example, if an international law enforcement agency caught a customer in its jurisdiction and found evidence that he had been communicating with five different Philippine OSEC traffickers, these might have been sent to Philippine law enforcement as five different referrals, or as a single referral, depending on the referring agency's policies and practices. Nonetheless, the data from these referrals can give us a rough understanding of customers of OSEC.

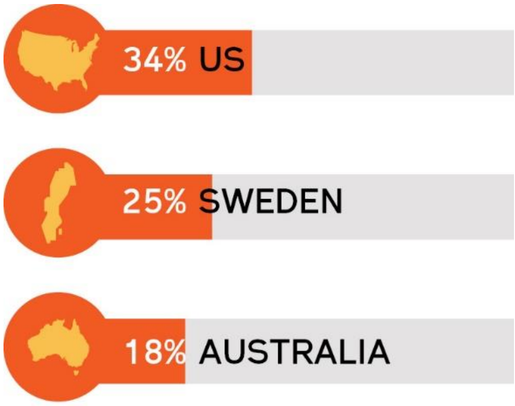
KEY FINDING #6

Customers tended to be older men.

All known customers were male. Fewer than half of all referrals contained data on the customer's age. Of the 18 referrals that did have information on the customers' age, most cases (56%; 10 cases) involved customers between 50-59 years of age, with the youngest customer age reported as 40 years and the oldest as 72 years.

KEY FINDING #7

Customers tended to be from Western countries, although many had traveled to or lived in the Philippines at some point in time.



Most cases referred to the Philippines involved customers from the United States (15 cases), Sweden (11 cases), and Australia (7 cases). Customers from the following countries were mentioned in one to three cases each: Canada, Ireland, Israel, the Netherlands, Norway, and the UK.[110] However, not all customers were based in their country of origin during the abuse. Two cases involved customers that were based in the Philippines while they were purchasing OSEC material, and five cases involved customers who moved back and forth between the Philippines and their country of origin during the abuse. However, customers in only two of these cases had a known history of contact abuse of children in the Philippines.

Regardless of customers' location during the time of abuse, about 39% of cases (17 cases) involved customers who were known to have traveled to the Philippines at some point in their lives, and 9% of cases (4 cases) involved customers with a known history of contact abuse of children in the Philippines.

OSEC Trafficker Typology

Traffickers are the people who provide, obtain, and recruit victims for customers, accept payment for the exploitation, and commonly commit or direct the contact abuse of the child for remote viewing.

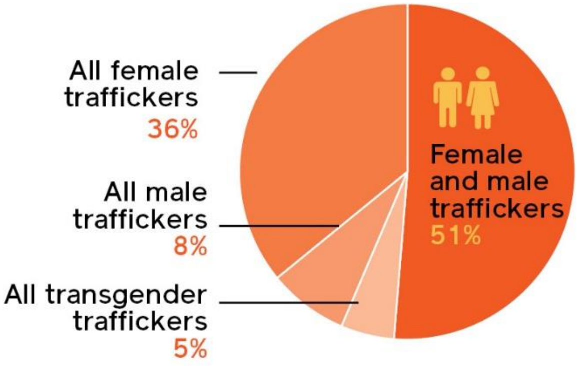
[110] These data likely tell us more about the way international law enforcement agencies find cases of OSEC and share information with Philippine law enforcement than about the number of customers that exist in each country.

KEY FINDING #8

There was an average of two traffickers per case.

Philippine law enforcement identified 141 traffickers in the 71 cases that they investigated between 2011 and 2017. That represents an average of two traffickers per case, with the number of identified traffickers per case ranging from zero[111] to 11. Of the 39 cases for which there were multiple traffickers, 51% (20 cases) involved mixed gender groups of traffickers, 36% (14 cases) involved all female traffickers, 8% (3 cases) involved all male traffickers, and 5% (2 cases) involved all transgender traffickers.[112]

FIGURE 9. Trafficker Teams



KEY FINDING #9

Traffickers tended to be younger Filipina women, often family members of the victims.

27 years old
96%

FEMALE

66% of traffickers were female.

MEDIAN AGE

Traffickers ranged in age from 15 to 76 years old.

FILIPINO

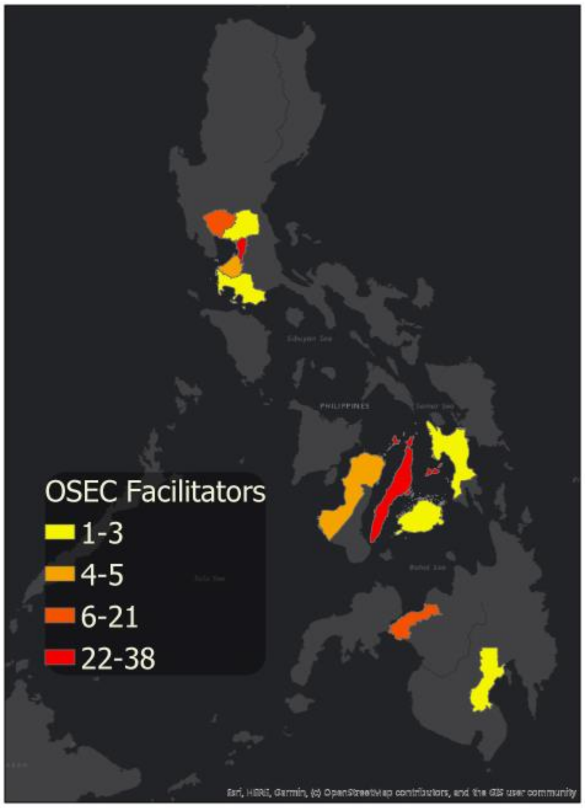
Only five traffickers were foreign nationals.

[111] Note: There are two situations in which a case may result in zero traffickers. First, the law enforcement investigation may fail to identify a local trafficker despite indications that one was involved. Second, the law enforcement investigation may positively determine that the child was used directly by the remote offender. RA 9208 as amended by 10364 prohibits, as a trafficking in persons offense, the "use…of a child…for the production of pornography, or for pornographic performances…" Therefore, even when no Philippine trafficker is identified, the foreign subject who communicated with and used the child to produce the CSEM is considered the trafficker for purposes of Philippine law. In that sense, the Philippine criminal justice system does not bring a trafficker before the court, but the child is still a trafficking victim without the involvement of a local trafficker.

[112] The term "transgender" is used to describe people whose gender presentation differs from the sex they were assigned at birth.

Traffickers ranged in age from 15[113] to 76 years old, but the median age was 27 years. More than 65% of traffickers (93 traffickers) were female, with another 31% (44 traffickers) being male and 3% (4 traffickers) being transgender. As noted previously, most traffickers were relatives of the victims. The vast majority of traffickers (97%; 136 traffickers) were Filipino, but five traffickers were foreign nationals from Australia, Japan, or the United States. As with victims of OSEC, traffickers of OSEC were found throughout the Philippines. As would be expected, traffickers usually lived in the same province as their victims. (See Figure 10.)

FIGURE 10. Heat Map of OSEC Trafficker Locations



Esri, HERE, Garmin, (c) OpenStreetMap contributors, and the GIS user community

The casework data available to the study team did not include statements, social histories, or other background details provided by arrested traffickers. This is due in large part to Philippine justice system restrictions on interviews of subjects under law enforcement investigation. Therefore, little is known about what factors influence traffickers to choose to engage in OSEC.

Observers may speculate that prior victimization – absent justice system driven rescue and intervention – may cause later OSEC criminality. However, the data do not support such a hypothesis. Based on the limited data available in case files, fewer than 5% (6 traffickers) of all traffickers were identified in the case files as former OSEC victims. Of the few victims-turned-traffickers that were identified, all were female, and half were 21 years old or younger. The ages of the other half were unknown. Given that OSEC has been widely acknowledged by law enforcement just within the past decade and the technology to facilitate OSEC has become more accessible in recent years, it makes sense that most victims-turned-traffickers were young. Given that this data was not intentionally collected in law enforcement case files, it is also possible that more OSEC traffickers were former victims and the data simply were not recorded. The study team does not suggest that a causal relationship between victimization and subsequent criminality exists. Rather, the study team calls for additional research to better understand if, how, and why early childhood abuse correlates to later OSEC offending, particularly within the Philippine social and cultural context.

[113] Note: Philippine law provides for minor offenders (less than 18 years of age) to be classified as children in conflict with the law (CICL) and receive non-criminal interventions under the custody of the Department of Social Welfare and Development.

FIGURE 11. Locations of Victims Rescued and Suspected Traffickers Arrested

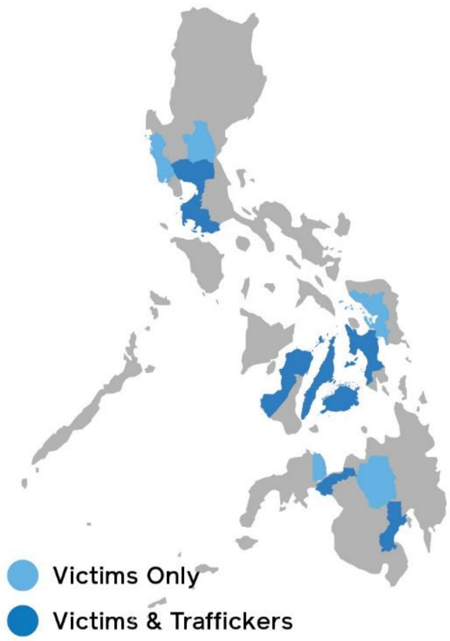


Figure 11 provides an overlap of the two heat maps from Figures 9 and 10. Notably, law enforcement has rescued victims in more areas than areas in which they have arrested suspects. This is indicative of a growing victim-centric approach to OSEC investigations, in which law enforcement appropriately prioritizes victim rescue and child protective actions, even when a timely arrest cannot be made.

OSEC Offending Process

The way OSEC is committed (e.g., what platforms are used to communicate or exchange materials/money, what materials are exchanged, and the cost of the materials) is jointly determined by the customer and the trafficker. In Philippine law enforcement investigations, the "customer" was usually an undercover investigator (UCI) posing as a customer online. To ensure that Philippine investigative processes are not confused with real customer's offending processes, information on the offending process was analyzed separately, based on the source of the data international law enforcement referral (64 cases) or Philippine law enforcement investigation (59 cases). Some key themes arose from both sources of data.

EN

ENGLISH

All traffickers communicated in English.

SURFACE OF THE INTERNET

Most traffickers communicated and exchanged materials with customers on the surface of the web (as opposed to the dark web).

FINANCIAL MOTIVATION

Evidence was able to confirm that there was a commercial element (e.g. exchange of CSEM for money) in 83% of all cases.

KEY FINDING #10

Most criminals who got caught communicated in English.

In both referral- and Philippine investigation-based datasets, all traffickers[114] communicated with the customer or UCI in English. This finding gives credence to anecdotal evidence from many anti-trafficking experts that the Philippines' large English-speaking population is a key enabling factor in the commission of OSEC. [115]

[114] This figure excludes the 33% of referral-based cases, for which there was no trafficker or for which the language of communication was not reported in the referral, and the 12% of Philippine investigation-based cases, for which the UCI and trafficker never communicated directly.
[115] Varella. (2017). Live streaming of child sexual abuse: Background, legislative frameworks and the experience of the Philippines. *ECPAT International Journal,* 12, 47-61.

KEY FINDING #11

The crime occurred on the surface of the internet.

Most traffickers communicated and exchanged materials with customers on the surface of the worldwide web (as opposed to the dark web). Often, they used platforms, such as social media or personal messaging sites, email, dating websites, or adult websites,[116] with basic privacy techniques, such as requiring a password, but did not use more advanced anonymization techniques.

In the 59 Philippine investigation cases,[117] only one trafficker was known to have used an anonymization technique, such as a VPN. For another 36% of cases (21 cases), law enforcement did not know if they used an anonymization technique. But in another 63% of cases (37 cases), traffickers were known to be operating without the use of any anonymization.

KEY FINDING #12

There appeared to be a financial motivation to the crime for most traffickers of OSEC. Evidence confirmed that there was a commercial element (e.g., exchange of CSEM for money) in 83% of all cases (49 out of 59 Philippine investigation cases and 53 out of 64 international law enforcement referrals[118]). Although the amount of money exchanged varied vastly from case to case, even the smallest exchanges were equivalent to days, if not weeks, of pay at the Philippine minimum wage.

[116] See Appendix E for details on which types of platforms were used for communication vs. exchange of materials.

[117] Referrals rarely, if ever, reported on the use of anonymization techniques, so this data was not collected for referral cases.

[118] Under Philippine law, the exchange of money or goods is not a required element in the criminal trafficking offense of CSEM production (including OSEC).

SPOTLIGHT Survivors of OSEC: What Do We Know?

A Philippines Aftercare Spotlight

IJM has assisted the authorities in the rescue of 571 children in 171 cases of OSEC in the Philippines as of the end of 2019.[119] In all these cases, IJM collaborates closely with the Philippine Government's Department of Social Welfare and Development (DSWD) and NGO partners to provide comprehensive, trauma-informed aftercare services, including collaborative case management, therapy, education and economic empowerment, and legal assistance.

What are the Aftercare Challenges?

As discussed in the OSEC victim typology section of this report, OSEC survivors largely represent a different demographic than survivors of street and establishment-based sex trafficking (CSEC). Over the previous two decades, the Government of the Philippines and private aftercare agencies developed a strong system of care for CSEC survivors, who were mainly comprised of girls in their late teens, but survivors of OSEC include more boys, younger children, and mixed-gender sibling groups. The unique nature of OSEC victimization poses challenges for the restoration[120] of young victims of the crime, in particular for those whose families or relatives were involved in the exploitation and abuse. In the Philippines, IJM and DSWD are collaborating closely to provide services for these survivors, challenges have been identified in the existing system of care that are being addressed at the individual, family, community and system levels.

When Philippine law enforcement identifies and removes children from situations of abuse, they are placed in the protective custody of the DSWD, the government agency responsible to care for children in need of special protection. IJM and its partners collaborate to ensure a trauma-informed approach to supporting OSEC survivors through the system; this includes victim-sensitive approaches during inquest and legal proceedings to reduce re-traumatization121 and strong collaborative case management through the recovery and reintegration process.

While there have been strong efforts to respond to the needs of OSEC survivors, there is still a need for expanded options for this demographic of children when they are placed in DSWD protective custody. Few residential care shelters will accept mixed-gender sibling groups and shelter placements for boys are quite limited. IJM-assisted OSEC casework has also included infants and toddlers. Aftercare options for this population are even more challenging as very young children may be more likely to experience positive aftercare outcomes in a family-based setting such as kinship or foster care; expansion of these care options is needed while children await reintegration.

[119] Note: this represents the totals for all OSEC casework IJM has supported from 2016 – 2019, so these numbers will differ from the totals included in the casefile review section of the report which is limited to the study years of 2010-2017.
[120] IJM defines restoration to be when a survivor is able to function in society with low vulnerability to revictimization.
[121] See Spotlight: Promising Practices in Prosecution on p. 68.

More critically, IJM and partners have found that the safe reintegration of children back into their communities and families of origin can pose many challenges. OSEC survivors often return into settings where family and community members tolerated or supported the crime without understanding or acknowledging the severe harm that OSEC causes. Reintegration without thorough safety assessments and support services in place for families and communities could leave children vulnerable to revictimization.

Survivors of child sexual abuse often experience complex trauma, which describes both exposure to multiple traumatic events (abuse, neglect, etc.) and the wide-ranging, long-term impact of this exposure.[122] Complex trauma can impact a child's development and wellbeing, including cognition, physical health, and the ability to form secure caregiver attachments and healthy peer relationships.

The complex nature of OSEC as a crime presents additional challenges to trauma recovery. This includes an unknown element of potential ongoing revictimization; there is no clear 'end' to the abuse when images and videos continue to recirculate on the internet accessible to an unknown number of perpetrators. This may make it difficult for a survivor to resolve or identify an end to the abuse.[123,124] The young age of many OSEC victims also makes disclosure of the abuse difficult. Not all survivors, especially very young children, are aware of what is happening to them during online exploitation or that they have even been exploited.[125,126] As noted, a large percentage of cases involve trafficking by family members, which results in care challenges when survivors are removed from their homes and placed in protective custody. When parents and family members are involved in the abuse, this results in confusion, betrayal, shame, and broken trust. Another layer of trauma involves child victims who may have been coerced or forced to engage in sexual contact with another child (including siblings) as directed to do so by a trafficker. Additionally, survivors often struggle with guilt when the abuser is a family member and is incarcerated, especially if they testified against them in the trial process.

Addressing the Challenges

Strengthened Alternative Care: As OSEC survivors are often young children and sibling groups who are removed from their homes and await permanent care solutions while under DSWD's protective custody, it is critical to ensure that systems of care follow best practices with the best interest of the child in mind. The United Nations promotes making an effort to keep a child in the care of their family/kin or, when that is not possible, in the "best alternative care" option while permanent care solutions are sought. The UN's Guidelines for the Alternative Care of Children state that alternative care for young children, especially those under the age of three years, should be provided in family-based alternative care settings. Alternative care includes informal and formal kinship care, foster care, and other family-like residential care placements. Siblings should not be separated by placements unless there is a clear risk of abuse or other justification in the best interests of the child.[127]. Strong assessments that take best interest of child and their needs into consideration are critical when considering alternative care placements for OSEC survivors, given the complex dynamics of the abuse.

IJM collaborates with the DSWD and other partners in the Philippines to follow these best practices to strengthen alternative care options for OSEC victims, including strengthening of the existing national foster care system to care for OSEC survivors and expanding assessment and placement options for boys and sibling groups, in order to protect children while permanent care solutions are found.

[122] *National Child Traumatic Stress Network. Complex trauma. Retrieved from www.nctsn.org/trauma-types/complex-trauma.*

[123] Leonard, Marcella Mary (2010). "I did what I was directed to do but he didn't touch me": The impact of being a victim of internet offending, *Journal of Sexual Aggression*, 16:2, 249-256.

[124] Martin, Jennifer (2014). "It's Just an Image, Right?": Practitioners' Understanding of Child Sexual Abuse Images Online and Effects on Victims, *Child & Youth Services,* 35:2, 96-115.

[125] United Nations Children's Fund (2011). *Child safety online: Global challenges and strategies.* Retrieved from https://www.unicef-irc.org/publications/650

[126] Martin, J. (2015). Conceptualizing the harms done to children made the subjects of sexual abuse images online, *Child & Youth Services, 36(4),* 267-287.

[127] United Nations. (2010). *Guidelines for the Alternative Care of Children.* Retrieved from https://www.unicef.org/protection/alternative_care_Guidelines-English.pdf

Family and Community-Based Reintegration Services: When possible, efforts are made to keep children in the care of their biological families or relatives. Engaging and strengthening community-based services, particularly for families of OSEC survivors who are reintegrating back into their communities, is critical to creating a protective environment for children. IJM and local partners coordinate closely to ensure strong family services and supports are available and accessible; specifically, parents of OSEC survivors have benefited from community-based psychoeducation services that build the capacity of families to strengthen protective factors for children that will support their restoration journeys and reduce the likelihood of revictimization.

Aftercare service providers must conduct strong home assessments and engage support services in the community that respond to the needs of both survivors and families; this includes multi-disciplinary, collaborative case management with strong follow-up, awareness-raising on child protection laws and accessing social services, and educating communities and families on the impact of OSEC as a crime on victims and the risk of prosecution for perpetrators.

Trauma-Focused Interventions

The impact of child sexual abuse is affected by the duration of abuse, severity of abuse, age of child when abuse occurred, and relationship with perpetrator of the abuse; for OSEC survivors, level of trauma will also vary according to these factors. Sensitive facilitation of disclosure conducted by trauma-informed, victim-sensitive professionals is critical in order to address trauma in children as they begin to understand what happened to them. When a survivor has experienced abuse by trusted adults, siblings, or relatives and/or has subsequently been placed in protective custody, a child faces additional complex trauma impacts; practitioners and caregivers should be equipped with interventions to rebuild trust and attachment between a child and adults, especially for younger children.

IJM and partners are investing in building the skills of service providers and practitioners to address these needs through improving trauma-informed care, strengthening trust and attachment-based interventions, and increasing access to trauma therapy resources. However, better understanding the complexities of the impact of OSEC, including the potential for recurring revictimization when abuse images recirculate online, is still a critical need in order for mental health professionals to address the risk of re-traumatization and to create or adapt existing trauma frameworks and treatment modalities to work with OSEC survivors.[128] As the Philippines Government and its partners are restoring OSEC survivors, they are collaboratively developing approaches that will be valuable tools for serving victims in other contexts; this include collaborative case management and the strengthening of a trauma-informed system of care that will address the needs of survivors from rescue to restoration.

[128] Martin, J. (2015). Conceptualizing the harms done to children made the subjects of sexual abuse images online, *Child & Youth Services,* 36(4), 267-287.

EXAMINING THE PHILIPPINES AS A GLOBAL HOTSPOT FOR OSEC

This section presents the results of two separate data collection/analysis efforts: one exploring global data on law enforcement OSEC cases that had been referred from one country to another; and one examining NCMEC data on CyberTipline reports that had been reviewed by NCMEC analysts, classified as involving incidents of "online enticement," and made available to more than one country's law enforcement. Both data collection efforts were focused on data from within the baseline time period (2010-2017).

KEY FINDINGS

1. According to global law enforcement data, the Philippines was the largest known source of OSEC cases.
2. The Asia/Pacific region was the third largest source of "online enticement" CyberTipline reports.

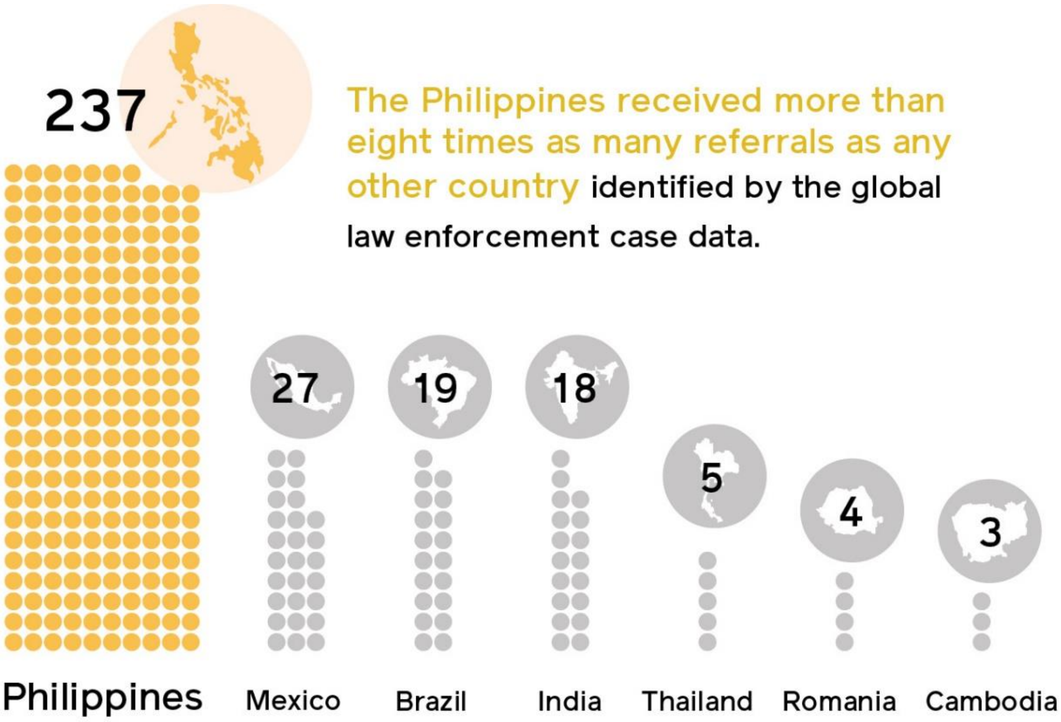
KEY FINDING #1

According to global law enforcement data, the Philippines was the largest known source of OSEC cases.

Four law enforcement agencies from around the world shared with the study team the total number of OSEC cases they referred to another country between 2010 and 2017. These agencies included the Royal Canadian Mounted Police (RCMP), the United Kingdom National Crime Agency (NCA), the United States Federal Bureau of Investigation (FBI), and the Nordic Liaison Office (NLO) representing Norway, Sweden, Denmark, Finland and Iceland.   The data on cases were then disaggregated by country to which the OSEC case was referred.

These data seemed to verify what OSEC investigators have long acknowledged — that the Philippines is an OSEC hotspot. The case data from the four global law enforcement agencies identified seven OSEC source countries between 2010 and 2017. (Figure 12 lists these OSEC source countries and shows the number of OSEC cases referred to each.) The Philippines received more than eight times as many referrals as any other country identified. As mentioned in the Methodology section, failure to appear on this list does not indicate that a country does not have an OSEC problem, but presence on this list is evidence of at least some incidents of OSEC.

FIGURE 12. OSEC Source Countries Identified by Global Law Enforcement Case Data



KEY FINDING #2

The Asia Pacific region was the third largest source of "online enticement" CyberTipline reports

The study team conducted an analysis of NCMEC CyberTipline reports classified as "online enticement of children" incidents involving activity in two or more countries. The international "online enticement" CyberTipline report data also support the idea that the Asia Pacific region is a major source of OSEC cases.

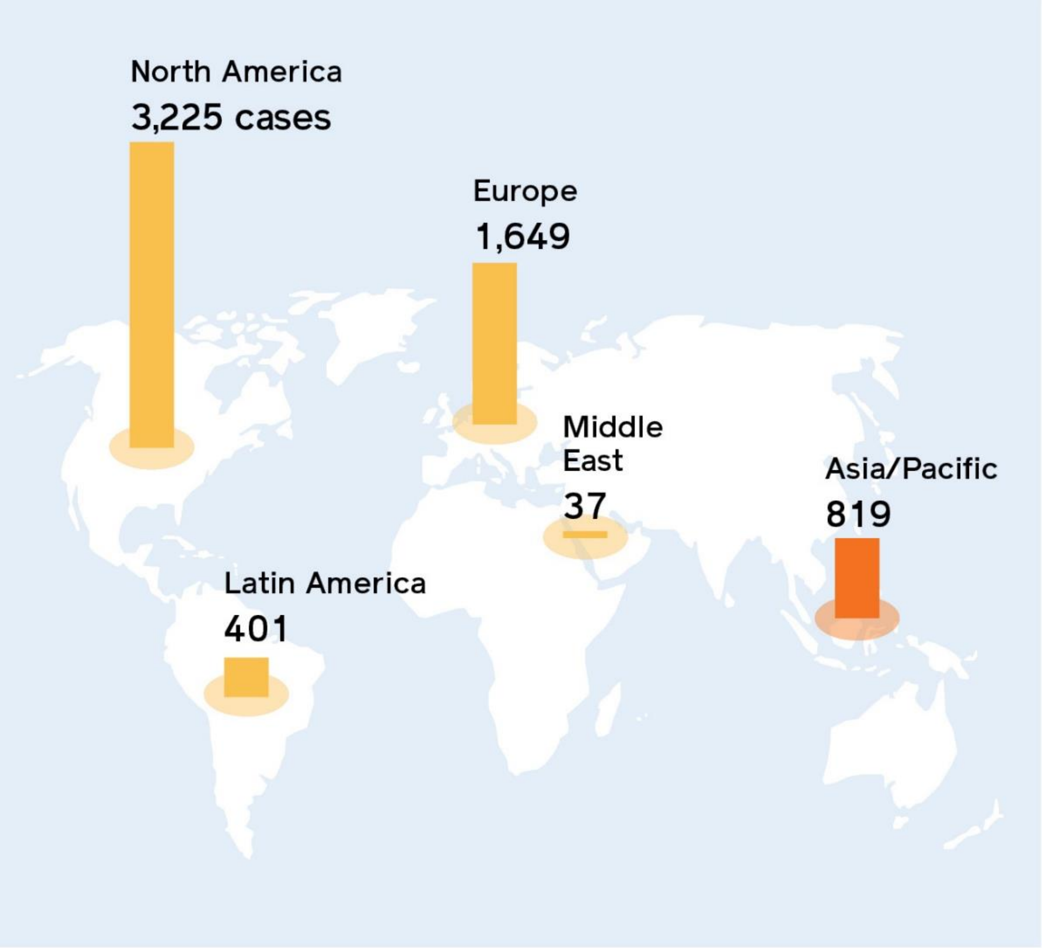
NCMEC identified 3,005 CyberTipline reports categorized as "online enticement" that had been made available to foreign law enforcement in more than one country between 2010 and 2017. The majority of these CyberTipline reports were made available to foreign law enforcement in two countries, but a handful were made available to foreign law enforcement in three or more countries.

Figure 13 lists all the regions to which "online enticement" CyberTipline reports were made available to law enforcement. The majority of CyberTipline reports related to "online enticement" (3,225) were made available to law enforcement agencies in North America. Europe had the second highest number (1,649) of multi-country "online enticement" CyberTipline reports. North America and Europe are known to be home to many OSEC customers but may have many OSEC traffickers and victims as well.[129] Asia/Pacific, the region in which the Philippines is located, had the third highest number (819) of multi-country "online enticement" CyberTipline reports globally. This region includes a mix of countries that may have a

[129] WePROTECT Global Alliance. (2018). *Global Threat Assessment 2018: Working Together to End Sexual Exploitation of Children Online.* Retrieved from: https://static1.squarespace.com/static/5630f48de4b00a75476ecf0a/t/5a83272c8165f5d2a348426d/1518544686414/6.4159_WeProtect+GA+report.pdf

combination of OSEC customers and traffickers or victims (Australia, New Zealand, Singapore, Hong Kong, South Korea, and Japan) and countries that likely have far more OSEC traffickers and victims than customers (Philippines, Thailand, Indonesia, Malaysia, Vietnam, and Cambodia).

FIGURE 13. Regions Receiving NCMEC CyberTipline Reports Involving Two or More Countries Related to "Online Enticement of Children"



Wrestling with the Key Findings

Overall, the data from all three parts of this study suggest that OSEC is a growing problem in the Philippines, perpetrated by a unique type of offender and affecting very young children. However, due to the experimental nature of the study design and significant limitations on the quality of the data available, there is room to critique and improve upon the approaches used in this report. Below is a discussion of the main findings, which includes the strengths and weaknesses of the results and alternate interpretations. The study team acknowledges that there is room to discuss and debate some of the conclusions, and we present this section as a start to that discussion.

Reports of OSEC and other forms of Internet-based CSE are increasing in the Philippines

The last decade has seen a dramatic increase in reporting of suspected CSEM sharing and OSEC in the Philippines, as evidenced by the following:

1. There were fewer than 50 Philippine IP addresses reported to NCMEC through CyberTipline reports in 2010 and 2011. But between 2012, when there was an initial spike in reporting, and 2017, there has been greater than 700% growth in the number of Philippine IP addresses reported to NCMEC through CyberTipline reports;
2. Prior to 2013, fewer than 3 OSEC cases per year had been referred to and/or investigated by PNP WCPC and NBI-AHTRAD. But from 2013 to 2017, the number of OSEC cases reported to these law enforcement agencies increased an average of 58% every year.

This increase in reporting could be caused by a few different factors. First, there has been an increase in recognition of OSEC as a crime, which has led to greater reporting to both NCMEC and law enforcement in general. Second, the growth in cases referred to PNP WCPC and NBI-AHTRAD has been supported by improved relationships between Philippine law enforcement and international law enforcement agencies, and increased confidence that Philippine law enforcement will responsibly investigate referrals. Third, the rise in reporting may be due to an actual increase in the number of offenders committing the crime. IJM investigative experts in the Philippines have witnessed and can confirm that the first two factors have impacted reporting over the past four years. However, whether the rise in reporting is related to an actual increase in offending is harder to determine.

The mark-recapture analyses presented in this study support the idea that there has been a true rise in the number of IP addresses used for CSE in the Philippines. In 2014, the annual estimate of the number of Philippine IP addresses used for CSE was 23,333 (95% CI: 22,314-24,352); but by 2017, that number grew to 81,723 (95% CI: 80,188-83,259). This represented 250% growth in the prevalence of IP addresses used for CSE over a four-year time period. However, mark-recapture methodology is inherently affected by the number of "captures," or reports, of internet-based CSE. When NCMEC reporting is very low, this methodology will tend to underestimate the size of the population, and as reporting increases, the methodology will lead to higher, more accurate estimates. During the study period, there was a 700% growth in NCMEC CyberTipline reports received containing IP addresses that resolved to the Philippines. However, global NCMEC reporting grew at an even faster rate. In 2010, NECMEC received 200,000 CyberTipline reports globally, and in 2017 they received 10.2 million CyberTipline reports — a 5,000% growth over the eight-year period. Therefore, it is unclear how much of the growth in the estimated number of Philippine IP addresses used for CSE is an improvement in estimate accuracy due to increased reporting versus an increase in the actual occurrence of Internet-based CSE in the Philippines. Further research is needed to understand how changes in NCMEC reporting affect the ability of mark-recapture analyses to create stable estimates of Internet-based CSE prevalence over time.

The true prevalence of OSEC remains unknown

The study team was not able to gain clarity on the percent of Internet-based CSE that is OSEC, so the study cannot draw any conclusions about the prevalence of OSEC. This was caused by significant variations in the types and quality of data ESPs provide to NCMEC in CyberTipline reports, which prevented the study team's criminal analysts from determining the OSEC status of around 80% of the CyberTipline reports they reviewed.

This lack of a finding was not altogether unexpected. When IJM originally convened stakeholders to discuss potential OSEC prevalence study methodologies in 2016, multiple experts warned the study team that the open-text data within CyberTipline reports are quite varied in terms of their quality and types of information they contain. Nevertheless, the study team conducted this data collection effort in an attempt to glean as much available data as they could.

The team's experience reviewing open-text CyberTipline report data identified some key problems in the way ESPs report internet-based CSE to NCMEC. For example, many ESPs have their own template for reporting CyberTipline reports, and each ESP's template is different. This reduces the quality and completeness of NCMEC CyberTipline data and renders a massive data set, with high potential for informing the field, less useful from a research perspective. Another issue identified through the data collection effort was that the criminal analysts did not identify a single incident of livestreaming OSEC in the CyberTipline reports, despite the fact that Philippine law enforcement case data show that livestreaming abuse is common in OSEC cases. The stakeholders on this study suggest that the livestreaming aspect of OSEC is not observed in NCMEC CyberTipline reports because ESPs do not yet have the algorithms to automatically scan video images as they can still images. The criminal analysts did identify a couple of highly suspicious reports in which chat logs indicated that the users intended to switch to a different platform to begin a video chat. However, because there is not currently a way for ESPs to coordinate reporting when users switch platforms, information about what happened in the video chat was not available for review. These are critical gaps in the field.

Further research is needed to design a methodology that can effectively measure the prevalence of OSEC and other types of Internet-based CSE. This research will likely need to be supported by new technologies and collaborations to improve the way ESPs identify and report Internet-based CSE. Until such technologies and collaborations are established, any efforts at measuring the prevalence of sub-types of Internet-based CSE are likely to be unreliable and fraught with measurement error.

The typology of OSEC traffickers is unique

This study found that the majority of OSEC cases (87%) involved at least one female trafficker, usually a mother or other female relative. This typology is quite unique in crimes involving sexual abuse/exploitation of children. Cases of child sexual assault commonly involve perpetrators who are family members, but they are typically males.[130] Based on IJM's Philippine case data, cases of establishment-based commercial exploitation of children (CSEC) sometimes involve female perpetrators (e.g., madams in brothels), but rarely are family members involved in the abuse. The study team hypothesizes that, like female traffickers in CSEC cases, female traffickers in OSEC cases are financially, not sexually, motivated to commit the crime. Literature also notes that OSEC traffickers often rationalize their crimes by saying that they are not causing

[130] Snyder. (2000). Sexual assault of young children as reported to law enforcement: Victim, incident, and gender characteristics. A NIBRS Statistical Report. Washington, DC: U.S. Department of Justice, Office of Justice Programs. Retrieved from: https://www.bjs.gov/content/pub/pdf/saycrle.pdf

real harm to their child because the abuse primarily happens online.[131,132] However, more research is needed to understand how and why OSEC traffickers begin committing this crime.

Furthermore, most cases (54%) involve more than one trafficker. Based on the experience of IJM and their Philippine law enforcement partners, in multi-trafficker cases, traffickers often have distinct roles. For example, one person may communicate with the customer while the other oversees or commits the sexual abuse or collects the money for the abuse.

All this may create unique challenges for survivor aftercare. When family members are directly involved in the abuse, Social Services often has fewer options for placing the survivor in care because family-based care may be unsafe. Furthermore, if the parents are arrested, there may be additional children beyond the survivor (e.g., brothers and sisters who were not abused) that also have to be placed in new homes. Beyond the logistical challenges of child placement, children who survive OSEC at the hands of their parents, as well as their displaced siblings, may experience more complicated trauma than children who are abused by people outside their families. Additional research is needed to understand the impact of OSEC, especially the impact of having the crime committed by a female relative, on survivors.

OSEC customers tend to be older English-speaking men from developed countries

All customers identified in this study were from developed countries. This is not surprising given the finding that in most cases (83%) traffickers appeared to be economically motivated. Although the amounts of money exchanged were sometimes surprisingly low, they were still the equivalent of days or weeks of a Philippine minimum wage. Most developed countries have a higher minimum wage than the Philippines, so there are vastly more people who have the means to afford to purchase OSEC than there are in the Philippines.

Previous studies have found that the age of customers ranges from mid-twenties to sixties, with no significant difference in ages across online-only and contact offenders.[133] However, this study did not identify any customers under the age of 40, and most customers were in their fifties. The study team found this somewhat surprising, given that technology can often be a barrier to entry into online crimes for older individuals. There are a few potential reasons for this. First, it may be that OSEC is not a technologically complicated crime to commit. It often involves the use of mainstream tools and platforms that do not require a great deal of sophistication to use. Second, it may be that younger customers are more tech-savvy and better at anonymizing themselves online, making them harder to catch. Third, it may be that younger men are more likely to engage in the higher-risk contact abuse, whereas older men may choose to engage in online abuse under the assumption that they are less likely to get caught. Finally, this could simply be an anomaly in the study data since only about half of the case referrals included data on the age of customers. More research is needed to understand *who* is purchasing OSEC and *why*.

[131] Ramiro, L. S., Martinez, A. B., Tan, J. R. D., Mariano, K., Miranda, G. M. J., & Bautista, G. (2019). Online child sexual exploitation and abuse: A community diagnosis using the social norms theory. *Child Abuse & Neglect*, *96*. https://doi-org.proxy.lib.fsu.edu/10.1016/j.chiabu.2019.104080

[132] Terre des Hommes (2013). Netherlands, November 2013 *Fullscreen on View – An Exploratory Study on the Background and Psychosocial Consequences of Webcam Child Sex Tourism in the Philippines.* Retrieved from www.terredeshommes.nl.

[133] Behaviour and Characteristics of Perpetrators of Online-facilitated Child Sexual Abuse and Exploitation

English is the language used to perpetrate OSEC

All traffickers identified in this study[134] communicated online in English. This makes sense since many anti-trafficking experts have identified the Philippines' large English-speaking population as a key enabling factor in the commission of OSEC.[135]

However, the anecdotal findings from the criminal analysts' review of open-text fields within CyberTipline reports indicated that Filipino and Tagalog were the primary languages used in 71% of chat logs reported to NCMEC. Although the OSEC status of most of those CyberTipline reports could not be determined, the study team believes that the Filipino- and Tagalog-language chat logs are unlikely to be incidents of OSEC. Rather, they likely represent some other form of in-country sexual abuse and exploitation. The bulk of the evidence from this study, as well as the experience of IJM OSEC investigation experts, suggests that OSEC cases typically involve international customers communicating with traffickers in English.

While hidden in homes, OSEC occurs on the surface of the internet

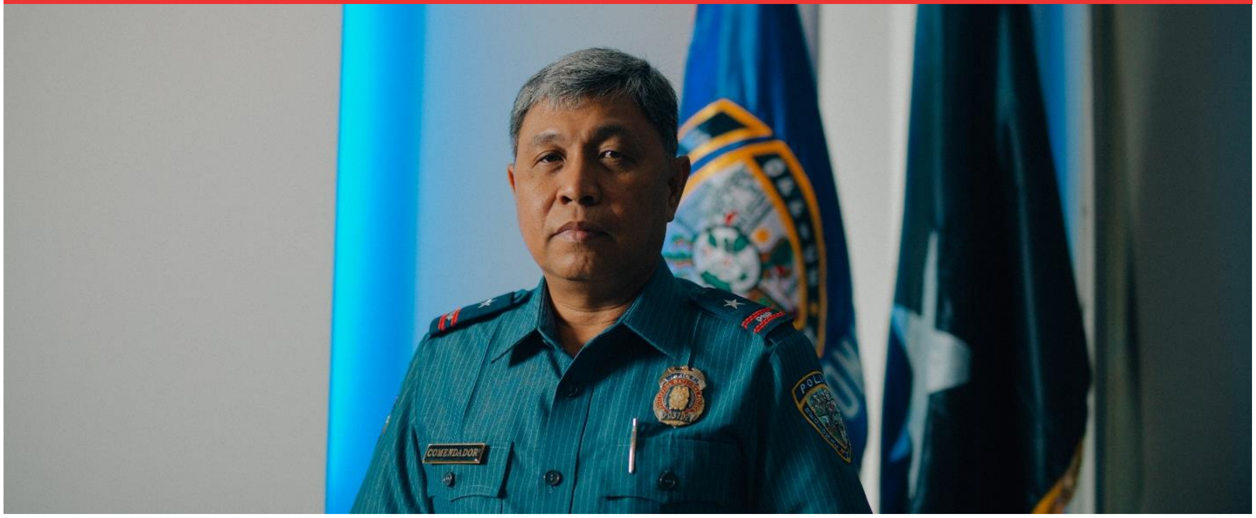
Traffickers identified in this study tended to communicate and exchange CSEM/CSAM with customers in a relatively non-secure way. They used platforms (e.g., social media, email, dating websites, etc.) with minimal security features to identify, communicate, and exchange materials with customers. Thus, the study team concluded that, during the study period, OSEC was conducted in relatively public online spaces — that is, on the surface of the internet on platforms created, and typically used for, licit communication.

However, this does not mean that OSEC *only* occurs in public online spaces. Incidents of OSEC occurring almost exclusively on the dark web or using high-tech anonymization tools may not have been captured by this study simply because they are less likely to get caught. Indeed, the study team believes that this crime *is* likely happening on the dark web. But right now, traffickers feel free to commit the crime on the surface of the internet. There may be a few causes for this. First, there are more potential customers on the open web, and many would-be traffickers can easily find customers there. Second, traffickers may perceive that they have a low risk of being caught and convicted of OSEC. Third, traffickers may not be technologically sophisticated enough to know about online privacy/security measures they can take.

[134] This figure excludes the 33% of referral-based cases, for which there was no trafficker or for which the language of communication was not reported in the referral, and the 12% of Philippine investigation-based cases, for which the UCI and trafficker never communicated directly.

[135] Varella. (2017). Live streaming of child sexual abuse: Background, legislative frameworks and the experience of the Philippines. *ECPAT International Journal,* 12, 47-61.

SPOTLIGHT Promising Practices in Prosecution



The typology of OSEC victims, as highlighted in greater detail in this report, poses significant challenges in the trial process, both in safeguarding the well-being of survivors as well as in ensuring successful trial outcomes. IJM's casework experience has shown that requiring children to recall and relay experiences of abuse during trial puts them at risk of re-traumatization. Additionally, the younger age of OSEC victims tends to impact their ability to testify to the facts of their case, and often more challenging — many cases involve a familial relationship with the OSEC traffickers, making testifying against their abusers all the more difficult for child victims. For this reason, IJM has constantly advocated for measures that will prevent child victims from having to actively participate in criminal trials and has identified several promising practices in this field.

Plea Agreements

A plea bargain, or a plea agreement, is a measure allowed by law in the Philippines that can result in a child being protected from relaying traumatizing experiences in open court. Plea bargaining has been found to be an effective method to resolving trials, as OSEC traffickers plead guilty to a lesser offense (in the Philippines, this often involves reducing an offense from Qualified Trafficking in Persons, which carries an automatic life sentence, to Trafficking in Persons, which carries a sentence of 15 years). Use of plea agreements can reduce the number of times a child is required to testify and reduce re-traumatization through the court process. Months of protracted legal proceedings can be shortened, providing the child survivor a sense of swifter justice. From the start of the IJM's OSEC program in 2011 through the end of 2019, the total count of convictions has reached 76, with 63 of those (83%) achieved through plea bargaining and 13 of those by full trial (17%). Plea agreements in OSEC cases have been found to significantly shorten trial lengths, improve prosecution outcomes while still providing meaningful sentences for perpetrators, and protect child survivors from additional trauma.

Video In-Depth Interviewing - VIDI

Another promising practice identified in IJM's OSEC casework thus far is the use of video interviewing. This reduces the number of times a child must provide testimony, can prevent the need for a child survivor to testify in front of their abuser, and reduce re-traumatization through the trial process. This protection measure in the Philippines is called Videotaped In-depth Interview, or VIDI, and the strategy finds basis in Section 29 of the Rule on Examination of a Child Witness (RECW). The Rule allows the admissibility of a child’s disclosure captured through a recorded video provided the Rule’s conditions are met. Through a VIDI, a child victim makes factual disclosures in a safe environment. Once secured on video, it may be used to replace the child’s actual presence, and even testimony, in the following situations: (1) during inquest or preliminary investigation before the prosecutor, and (2) at trial before a court. Through the VIDI, a child victim may be spared from repeatedly relaying abusive experiences.

IJM has been working with justice system partners to mainstream this prosecution strategy. In our collaborative casework to combat OSEC, we have seen increased utilization of VIDIs in Luzon, Visayas, and Mindanao. IJM has supported 53 cases with 111 instances of video-captured child interviews. Inquest prosecutors used 81% of these recorded interviews, protecting 90 children from potential re-traumatization and re-victimization.

Ideally, VIDIs are conducted in specialized child interview centers such as hospital-based Child Protection Units in the Philippines. However, the nature of OSEC crimes occurring in often remote locations has shown that this is not always possible. Interviews often must be conducted outside of interview centers and closer to the victims' communities. In light of this, IJM has developed a Mobile VIDI Kit and made kits available to government partners. Kits are composed of:

- Video Camera
- Tripod
- Laptop
- Storage Media (USB drives and SD cards)

Through the Mobile VIDI Kits, court-admissible, child-friendly interviews can be conducted even in areas where an interview center is not available. It is our hope that these kits will allow for the mainstreaming of this child-protective measure.

Specialized Training – POSE

IJM has found that, due to the technical nature of the crime and the very young victims involved, the successful prosecution of OSEC offenses can require specialized training for prosecutors and judges on topics such as court admissibility of digital evidence and the application of child protective measures in OSEC trial proceedings. To address this need, the Prosecuting Online Sexual Exploitation (POSE) training was developed as a product of partnership between the Philippine Inter-Agency Council Against Trafficking (IACAT), the U.S. Department of Justice, and IJM. The faculty includes experts on digital investigative analysis and prosecution from the Philippines and the United States. POSE's objective is to support law enforcement and prosecution frontliners in their casework through application-based training. As of December 2019, 79 prosecutors and 45 law enforcers have received this training.

The POSE trainings have been successful in improving trial outcomes and generating convictions in OSEC cases. From the first POSE training held in March 2018 through the end of 2019, there have been a total of 31 convictions secured by POSE-trained prosecutors. Apart from increasing competency in handling digital evidence, there were also opportunities to advance child-protective strategies in the prosecutorial system. One of these strategies is plea bargaining – a measure allowed by law through which the child is protected from having to relay traumatizing experiences in open court, as discussed above. Many POSE-trained prosecutors have become champions of plea bargaining. Notably, in the Philippines, Iligan City's Fiscal Jasmin Diaz, who attended both POSE 1 and 2, can be attributed with securing more than half (17) of these 31 OSEC convictions through plea bargaining. Cebu's Fiscal Rosemarie Pabatao, who attended POSE 1, was able to secure 9 of these OSEC convictions, also through plea bargaining.

IJM has found that application-based training for prosecutors on the more challenging aspects of OSEC prosecutions, including the use of digital evidence in court, video-taped interviews, plea-bargaining, and other child protective measures allow prosecutors to gain experience in implementing effective practices, which can result in more effective OSEC prosecutions overall.

Recommendations and Conclusions

This study's findings can be used by policymakers, practitioners, and others seeking to combat OSEC by informing interventions targeting this crime. Better understanding the scope and nature of the crime helps in improving law enforcement responses and social services for OSEC survivors. Below are some initial recommendations based on the study data and the experience of the study partners.

Many recommendations stemming from this research align with the WePROTECT Model National Response.[136] Where applicable, recommendations that align with the Model National Response capabilities needed for effective child protection are noted below the recommendation with a reference to the corresponding capability.

Recommendation #1:

The Philippine Government should continue scaling up the staffing and budget for its anti-trafficking law enforcement units, until they reach authorized levels at a minimum.

This study cannot definitively connect the rise in reporting of OSEC to law enforcement or the growth in Philippine-based NCMEC CyberTips to a rise in actual incidences of OSEC. Nevertheless, the increase in reporting of OSEC crimes to law enforcement suggests the need for additional resources to support Philippine anti-trafficking units. The government has already begun to respond to this need. Between 2016 and 2019, the Philippine government increased the annual operational funding for PNP WCPC by 246% and more than doubled the number of PNP WCPC staff. This is an excellent start. But given the large scale of the crime and the sustained sharp rise in reporting, it is recommended that the government continue increasing PNP WCPC staffing and budget until they have reach authorized levels and provide similar scaled-up resourcing to NBI-AHTRAD.

Model National Response Capability 4

Recommendation #2:

International and Philippine law enforcement agencies should maintain and build on the improved relationships and communication practices that exist between them to better hold perpetrators accountable and decrease criminal impunity globally.

The Philippine culture puts a high value on relationships. Many rules, which outsiders might label as "bureaucracy," are created to define and guide working relationships, but interpersonal relationships can help to break down bureaucratic barriers, accelerate work, and increase effectiveness. One example of such collaboration is the 2019 establishment of the Philippine Internet Crimes Against Children Center (PICACC), a joint initiative of the PNP WCPC, NBI–AHTRAD, UK NCA, Australian Federal Police, and IJM. Investments of time, resources, and expertise by the UK and Australia have helped strengthen trust and communication, with positive impacts on OSEC investigations and systemic enhancements.

Many foreign law enforcement agencies have liaison officers based in Southeast Asia, often with a broad range of thematic and geographic responsibilities within their assigned portfolios. However, due to the volume of OSEC originating from the Philippines and the need for strong collaboration to effectively address the issue, law enforcement agencies representing demand-side countries should assign liaison officers – specifically focused on child sexual exploitation

[136] *WePROTECT Global Alliance. (2016). Preventing and Tackling Child Sexual Exploitation and Abuse (CSEA): A Model National Response.*

matters, if possible – to live and work in the Philippines. Through relationships of collaboration, dedicated liaison officers can help ensure that investigative referrals get to appropriate operational units, additional support is offered and directed where it is most needed, and opportunities for successful casework outcomes are maximized. Additionally, longer rotations for these officers will support continuity and depth of relationships.

The Philippine government can support relationship-building with foreign law enforcement agencies by revising rules, which currently allow only executive leaders to communicate with foreign officials, to allow operational investigative staff to informally collaborate with foreign law enforcement agencies to advance OSEC casework.

Model National Response Capability 4

Recommendation #3:

International and Philippine law enforcement agencies should ensure OSEC cases are routed to one of the Philippine anti-trafficking units (PNP WCPC and NBI-AHTRAD).

The online sexual exploitation of children to create CSEM/CSAM in exchange for compensation is a trafficking offense under Philippine law. Although multiple crimes are committed in these offenses (e.g., sexual abuse of a child, cybercrimes, etc.), the study team recommends that OSEC be considered first and foremost as a trafficking-in-persons offense for two reasons. First, qualified trafficking carries a stronger possible penalty than the other criminal violations. Therefore, charging OSEC traffickers with trafficking (vs. another related crime) could create a stronger deterrent effect. Second, considering OSEC as a trafficking offense acknowledges the unique challenges and trauma of children who have been trafficked. Because anti-trafficking units focus on this specific crime type, they can gain more specific knowledge and experience to help them guard the dignity of trafficked children and effectively resolve their cases. PNP WCPC and NBI-AHTRAD are the Philippine law enforcement units best trained, resourced, and legally obligated to investigate trafficking crimes. Thus, all OSEC cases should be routed to these units to maximize the likelihood that (1) the case will be effectively investigated; (2) the traffickers will get a strong sentence; and (3) the dignity of the children who have been victimized will be protected. The most effective route to send OSEC referrals to these anti-trafficking units is through the PICACC, where new cases are reviewed by representatives from each partner agency on a weekly basis, and case assignments often are accompanied by offers of mutual aid to support casework outcomes.

Model National Response Capability 4

Recommendation #4

Government and non-government service providers should ensure a collaborative, trauma-informed, appropriate and holistic system of care exists to address the unique needs of OSEC survivors on an individual, family, and community level.

In the Philippines, the younger age of children, the high percentage of perpetrating family members, and the complicity of community members in OSEC presents challenges to existing systems of care for survivors of the crime, particularly in reintegration. These challenges, coupled with the complex trauma that survivors of OSEC experience, require a trauma-informed, appropriate, and holistic set of care options that address the needs of OSEC survivors and reduce the likelihood of revictimization. IJM and its government and non-government partners[137] are collaborating to ensure that there is a strong trauma-informed system of care that: ensures collaborative case management for individuals through the continuum of care from rescue to reintegration; provides secure and safe alternative care options for survivors who are removed from their biological families; addresses the immediate and long-term trauma impacts endured by victims of OSEC; and strengthens family and community-based services so that a survivor can reintegrate safely back into their families with a reduced risk of revictimization. Based on lessons learned while providing case management support to hundreds of OSEC victims in the Philippines, our team recommends that service providers gain a comprehensive understanding of the characteristics, vulnerabilities, risk, and resiliency factors of children, families, and communities impacted by OSEC in their contexts in order to inform recommendations for a robust system of care that will address the needs of these survivors.

Model National Response Capabilities 8 and 9

Recommendation #5:

Child protective measures and trauma-informed care should be implemented throughout the prosecution process of OSEC cases to protect victims from re-traumatization.

The typology of OSEC victims as detailed in this report can cause significant challenges in the trial process, particularly in safeguarding the well-being of survivors while ensuring successful trial outcomes. Thus, prosecutors and other justice system officials should ensure that child protective measures are employed throughout the justice system process as much as possible. These measures include reducing the reliance on victim testimony in court, use of child sensitive video interviewing, and consideration of plea agreements to achieve convictions with reduced trauma to survivors.

In the Philippines, the policy of the law is to protect the best interests of the child at every stage of legal proceedings. The use of plea agreements to secure convictions and spare children from testifying against their parents, relatives, or trusted adults, honors this policy and should be maximized in accordance with law. Measures under the Rule on Examination of a Child Witness, including video-taped in-depth interviews, live-link testimony, and video depositions, should likewise be used to minimize victim re-traumatization at the inquest, preliminary investigation, and trial stages.

Model National Response Capabilities 5, 8, and 9

Recommendation #6:

Technology platforms should identify and implement means for proactive detection of livestreaming OSEC.

The research team understands that the relative scarcity of apparent live-streaming OSEC offending visible in CyberTipline reports is a result of two key factors: (1) the widespread use of PhotoDNA and other hashing technologies to detect and report previously categorized CSAM, resulting in millions of CSAM-related CyberTipline reports; and (2) the lack of similar technologies developed and deployed on major tech platforms (during the study period) to detect newly created CSAM, whether in a saved image or video file or in a live video

[137] IACAT & DSWD

stream. Existing CSAM detection technologies like file hashing and PhotoDNA do not, and cannot, detect newly produced CSAM. Therefore, it is likely that the vast majority of instances of livestreaming remain undetected, unreported, and uninvestigated.

The tech sector, especially major tech platforms, should recognize the threat that undetected livestreaming exploitation presents to vulnerable children and choose to develop and deploy new technologies – including computer vision and machine learning applications of artificial intelligence – to detect newly produced CSEM in all its forms, including in live video streams. Innovative technological solutions will lead to increased detection and reporting.

When weighing user privacy against possible detection of child exploitation, tech platforms should elevate the privacy interests of victimized children over those of platform users, and prioritize detection of all, but especially newly produced, CSEM.

Model National Response Capabilities 16, 18, and 19

Recommendation #7:

Entities from across sectors should collaborate to strengthen processes to identify and report potential OSEC activity.

Indicators of OSEC-related activity include more than the exchange of CSEM material, and these additional indicators can be found on platforms across sectors ranging from social media platforms to cloud storage services to money transfer agencies. Taken alone, any one such indicator would be insufficient to even raise suspicion, much less confirmation, of live-streaming OSEC offending. However, it is reasonable to perceive an individual's likelihood of offending to be much greater when multiple indicators involving the same user are present and recognized, even across platforms or datasets. Tech companies, money transfer agencies, and NGOs should collaborate to recognize indicators of OSEC offending on their platforms and cross reference datasets from other entities to improve detection of likely offenders and report criminal conduct as appropriate. This type of cross-sector collaboration can both protect ESPs' systems against Terms of Service violations and criminal misuse and can serve to strengthen identification and reporting of suspected livestreaming OSEC.

Model National Response Capabilities 18 and 19

Recommendation #8:

Reporting of suspected CSEM on ESP platforms should be expanded and strengthened through mandatory reporting legislation in all States and the provision of higher quality information in reports.

In alignment with the 2018 Child Dignity Technology Working Group Alliance recommendations, all States should enact national legislation requiring ESPs to detect, report and speedily remove CSEM. Additionally, this research highlights the challenges that law enforcement and mandated agencies encounter in dealing with a high volume of reports that contain very little information. Therefore, ESPs should internalize responsibility in ensuring protection of children on their platforms and report any available associated information as *allowed* by law, rather than the minimum amount *required* by law. By providing more complete information, ESPs can help remove obstacles to effectively identifying offenders and victims. Furthermore, higher quality data will allow ESPs, law enforcement, and others to better identify and respond to concerning issues and trends.

Model National Response Capabilities 12, 16, and 17

Recommendation #9:

OSEC-related data owners, academics, technology designers, and OSEC experts should collaborate to conduct more research, increase our global knowledge about OSEC, as well as build the global stakeholder community's capacity to measure prevalence of the crime and impact of key interventions.

The study team titled our discussion of results as "Wrestling with the Key Findings" because we acknowledge that our data had limitations and the study identified as many new/remaining questions as it answered. We commenced this study because of the absence of quality study methodologies to understand this crime and hope that this baseline will provide lessons learned and a common pool of data to fuel future studies and improved methodologies. Some of our questions include:

- What is the prevalence of OSEC (vs. CSEM sharing)? In the Philippines? Globally?
- How and why do OSEC traffickers, especially mothers of victims, turn to this form of criminality? How is the psychological profile of this type of criminal distinct from or similar to others?
- What happens in the lives of OSEC victims before law enforcement gets involved? Do they disclose or show symptoms of the abuse? How are they conditioned for the abuse by their trafficker?
- What is the long-term impact of OSEC on survivors? Does this differ based on their relationship to their trafficker or the age at which they are rescued? What are the long-term-impacts on survivors of the recirculation of images on the internet?
- Who are the OSEC customers and what is the relationship between online and contact abuse from the offender perspective?
- On average, how many OSEC customers does each trafficker interact with? How many OSEC customers come from countries where law enforcement is not actively addressing the demand side of OSEC? How many/how often do customers travel internationally to abuse a child in-person?
- How does OSEC fit into the broader context of violence against children? What is the relationship between OSEC and other manifestations of violence against children for both offenders and victims?

This is the nature of OSEC: it involves hidden populations, with potential customers, traffickers, and victims spanning the globe, all with the ability to connect to one another—hardly ideal for developing a clean sampling frame that can yield generalizable results. The research team believes that this study has provided some new evidence to guide efforts to fight OSEC. But we also hope that this study will serve as a launching pad for the development of new research designs that can better answer some of the research questions we asked.

To do that, the anti-OSEC community will need to work together with academics, technologists, and the owners of various types of OSEC-related data, including law enforcement, reporting platforms/hotlines, money transfer agencies (MTAs), social media sites, and more. For example, law enforcement agencies could share with MTAs data from their cases on how much customers pay for OSEC. Working together, they may be able to define a money transfer profile of OSEC customers and traffickers that could both help law enforcement officers identify offenders faster and help researchers better understand the offending patterns of perpetrators. IJM and its study partners invite others to critique and build on any of the methods presented in this report or to innovate from scratch to help the field better understand this crime.

However, this research has also highlighted the need for future attempts to measure the prevalence of OSEC to be supported by new technologies and collaborations that improve the way ESPs identify and report internet-based CSE. Until such technologies and collaborations are established, any efforts to measure the prevalence of OSEC (or other sub-types of internet-based CSE) are likely to be unreliable and fraught with measurement error. Thus, we recommend that the field focus its resources and efforts, not on repeated attempts to measure OSEC prevalence, but on creating those new technologies and collaborations and on conducting qualitative studies to better understand the nature of these crimes, which can guide stakeholders in their efforts to fight OSEC.

Model National Response Capability 2

Recommendation #10:

All stakeholders should contribute toward an increase in international and cross-sector collaboration to protect children from online exploitation.

This study highlights both the global nature of OSEC crimes and the corresponding global spread of stakeholders the crime touches from social media platforms, money transfer agencies, law enforcement, NGOs engaged in responding, etc. This diversity, both geographically and across sectors, presents challenges in understanding the crime, identifying indicators and instances of it, and developing comprehensive responses to target it. A global crime necessitates a global, coordinated response.

Thus, impacted or engaged stakeholders should increase their collaboration with others on this issue, sharing learnings, data, and best practices to improve the global community's ability to protect children online. Where applicable, stakeholders should (1) work with global bodies in this area such as the WePROTECT Global Alliance, The Virtual Global Taskforce, the Global Partnership to End Violence Against Children, (2) participate in and convene other local and global forums to share learnings and coordinate efforts across sectors, and (3) identify, resource, and implement innovative projects in cross sector collaboration.

Conclusions

Internet-based CSE, in general, and OSEC, specifically, appear to be rapidly growing crimes in the Philippines. The monthly number of IP addresses used for CSE increased nearly 10-fold between 2014 and 2017. OSEC victims tended to be very young children of both sexes, and OSEC traffickers tended to be female relatives of the victims. The crimes occur on the surface of the internet, on commonly used platforms meant for licit communication.

Though a perfect measure of the prevalence of OSEC was not found through this study's efforts, the findings will still be of value to guide programming and policy decisions to improve law enforcement responses to OSEC crimes and social services for OSEC victims. Nonetheless, additional research and improved estimates of the prevalence of OSEC are needed to better inform OSEC interventions in the future.

Appendices

Appendix A. Detailed Methodologies

Mark-Recapture Methodology

METHODS FOR THE MARK-RECAPTURE ANALYSIS

DATA SET UP

NCMEC provided the study team with a data set of all CyberTipline reports identifying Philippine-based IP addresses from the years 2010-2017, excluding CyberTipline reports related to viral/meme images.[138] The data set included 16 variables. (See Table 2 for a full list and description of the variables.)

TABLE 2. Variables Included in the NCMEC Data Set

Variable	Description
Report ID	CyberTipline report ID number
Report Date/Time	The exact time and date the CyberTipline report was submitted to NCMEC
Reporting ESP	The company that submitted the CyberTipline report to NCMEC, if the CyberTipline report was submitted by an electronic service provider (ESP)
Source	Source of report (e.g., bulk/automation from ESP; ESP report via API using automation; manually submitted report from ESP; unknown; other [e.g., citizen report])
NCMEC classification	If a CyberTipline report was reviewed by a NCMEC analyst, this variable was labeled with the report classification (e.g., "Child Images," "Online Enticement—Pre-Travel," "Suicide Threat"). If a CyberTipline report was not reviewed by a NCMEC analyst, this variable was labeled "Apparent Child Pornography—Unconfirmed International," "Auto-referred International," "Unconfirmed—Files Not Reviewed by NCMEC." Because NCMEC focuses on US cases and often auto-refers international cases to the relevant law enforcement agency without review, 98.5% of all Philippine-referred CyberTipline reports were not reviewed by a NCMEC analyst.
New Photo DNA	If positive, indicated that the report contained an image alert for possible new (e.g., not previously seen by NCMEC) file, based on PhotoDNA. This does not indicate whether the "new" file contains CSAM.
Law Enforcement Agency	All law enforcement agencies to which the report was made available
Reported Person Age	Age of the person being reported for inappropriate conduct, if known. This data was missing from 33% of CyberTipline reports. Even when it was reported, the data were considered unreliable because they were typically based on the birthdate the user provided when setting up their social media accounts, the veracity of which was unknown.
Victim Age	Age of the person being victimized, if known. This data was missing from 99.5% of CyberTipline reports.

[138] Note: Researchers chose to exclude CyberTipline reports related to viral/meme images because these are rarely cases of OSEC, as defined by the study. However, NCMEC was only able to exclude reports that were labeled as viral/meme images by the person/company who submitted the CyberTipline report to NCMEC. Many CyberTipline reports report viral/meme images but are not labeled as such by the reporting company. Because researchers had no way to identify CyberTipline reports reporting viral/meme images that were not labeled as such by the reporter, without manually reviewing each report, those CyberTipline reports were included in the final data set.

URL	The website on which the inappropriate conduct occurred
IP Address	The IP address identified in the CyberTipline report
Proxy	If positive, indicated that the IP address may be a proxy IP address (e.g., VPN)
ISP	The internet service provider (ISP) that owned the reported IP address
Organization	The organization that owned the reported IP address. (This was usually the same as ISP or was the parent company of the ISP.)

Each row in the original data set represented an entry for which all variables were unique. So, for example, if a CyberTipline report was associated with three IP addresses, there were three entries for that CyberTipline report in the data set, each with the same Report ID but a unique IP address. Similarly, if a CyberTipline report with one IP address was made available to multiple law enforcement agencies, the Report ID was repeated two times in the data set, each with a unique law enforcement agency, but with "NULL" for the IP address in all but the first entry. With all these duplicates, the initial data set consisted of 1,009,711 entries containing data about 129,077 unique CyberTipline reports.

Because the primary variables of interest were Report ID, IP Address, and Report Date/Time, all entries with missing data ("NULL" or "Unknown") in the IP Address variable were removed. (No entries had missing data for Report ID or Report Date/Time.) This reduced the data set to 524,854 entries. However, this data set still included many duplicate entries, so all redundant IP addresses were removed by day. This reduced the data set to 206,155 entries. In the final step of cleaning, all IP addresses that were not geolocated to the Philippines[139] were removed from the data set, leaving 193,405 entries.

No Philippine IP addresses were reported prior to late 2011, and very few were reported from 2011-2013. Because low levels of reporting create unreliable mark-recapture estimates, IP addresses reported prior to 2014 were removed from the analyses, leaving 183,184 entries in the data set, and estimates were created only for the years 2014-2017.

STATISTICAL MODELS

In its most basic form, mark-recapture methodology requires two important assumptions to be true in order to provide meaningful results: (1) The "marking" technique must not affect the marked individual's chances of survival or recapture; and (2) The population should be closed (e.g., no one enters or exits the population through birth, death, immigration, emigration, etc. between captures). It is unclear how well the NCMEC CyberTipline data conform to these assumptions. Although individual user accounts may be shut down if they are reported to NCMEC (which violates assumption #1), the IP address, itself, is unaffected and can continue to be used (which conforms to assumption #1). Similarly, while the population of internet users in the Philippines is constantly growing (which violates assumption #2), the number of IPv4 addresses[140] assigned to the Philippines has remained relatively steady since 2011. However,

[139] Non-Philippine IP addresses would be included in the data set if they were identified in a CyberTipline report along with Philippine-based IP addresses.

[140] IPv4 is the fourth version of the IP address system that identifies devices on the internet. It uses a 32-bit address scheme, allowing for about 4 billion unique IP addresses.

ISPs are transitioning to IPv6 addresses[141] to support the continued growth in internet users.[142] As of early 2018, IPv6 addresses made up about 7% of all IP addresses in the Philippines, but fewer than 20% of these IP addresses were available to the public.[143] Thus, it is difficult to determine how well the study conforms to assumption #2. Fortunately, because the behavior of human populations can be drastically different from the wildlife populations that the mark-recapture methodology was initially designed to study, statisticians have developed advanced models to adjust the method for open populations and varying survival probabilities between captures.

Because this is the first attempt (to the researchers' knowledge) to use a mark-recapture methodology to estimate the prevalence of OSEC, it was unclear which statistical models would produce the best results. Therefore, various statistical mark-recapture extrapolation models using different estimators, capture periods, and numbers of captures were applied, and the results compared across models.

Both closed and open population models and estimators were explored. The closed population estimators consisted of Chao's lower bound estimator based on the M_{th} model[144] and the sample coverage approach estimator.[145] The open population estimator is that presented in Cormack (1989)[146] and which is based on a loglinear model. Each model/estimator was applied to a mark-recapture setup based on three, four, five, and six sampling occasions where each sampling occasion comprised all unique IP addresses observed in the span of one week. This gave rise to 3x4=12 different estimates. Additionally, the open population estimator was applied to the annual data sets based on thirteen sampling occasions, where each sampling occasion comprised all unique IP addresses observed in the span of four weeks. In total, 13 different estimates were obtained.

In total, 13 different models were run, as summarized in Table 3. For the captures that spanned one week, each "capture" was created by listing all unique IP addresses reported in any given week between January 1, 2014 and December 31, 2017. For the three-capture models, three consecutive one-week "captures" were compared to see how many IP addresses were reported in more than one "capture." Models were run with each of the estimators to estimate the total number of IP addresses used for CSE in every three-week period of time in the study period. In the four-, five-, and six-capture models, this process was repeated, but instead of comparing three consecutive captures, four, five, or six consecutive "captures" were compared in each model, respectively. The results of these models were estimates of the number of IP addresses used for CSE in any given three-, four-, five-, or six-week time period during the study period (2014-2017).

For the capture that spanned four weeks, each "capture" was created by listing all unique IP addresses reported in any given *four*-week time period during the study period. Thirteen consecutive four-week "captures" (the equivalent of one year of time) were then compared to see how many IP addresses were reported in more than one "capture" during the year. Only the open population estimator was used for these analyses because, with the longer period of time being analyzed, there was more risk that the closed population assumption would be violated.

[141] IPv6 is a newer IP address system that is slowly being rolled out worldwide. It uses a 128-bit address scheme, allowing for trillions of unique IP addresses.
[142] Dalal. (March 2019). IPv6: Powering the Next-generation Internet. Retrieved from: http://philv6forum.org/blog/ipv6-powering-the-next-generation-internet/
[143] Mulingbayan. (March 2018). APNIC Update for Philippines. Retrieved from: https://www.slideshare.net/apnic/phnog-2018-apnic-update
[144] Rivest, L.-P. and Levesque, T. (2001). Improved log-linear model estimators of abundance in capture-recapture experiments. *The Canadian Journal of Statistics* **29**, 555-572.
[145] Chao, A. (1987). Estimating the population size for capture-recapture data with unequal catchability. *Biometrics* **43**, 783-791.
[146] Cormack, R. M. (1989). Log-linear models for capture-recapture. *Biometrics* **45**, 395-413.

The results of this model would be estimates of the number of IP addresses used for CSE in any one-year time period during the study period (2014-2017).

TABLE 3. Models to Estimate the Total Number of IP Addresses used for CSE

Estimator	Length of Capture Period x # of Captures				
	1 Week				4 Weeks
	3	4	5	6	13
M_{th} model with Chao's lower bound estimator	●	●	●	●	
Sample coverage estimator	●	●	●	●	
Open population estimator	●	●	●	●	●

For most one-week capture periods (regardless of whether three, four, five, or six capture periods were analyzed), the M_{th} model with Chao's lower bound estimator was found to be more robust than the sample coverage or open population estimators. Therefore, this report presents only the results from the M_{th} model with Chao's lower bound estimator for the one-week capture periods.

There was not a significant difference in goodness-of-fit between the three-, four-, five-, and six-capture models. Therefore, for simplicity of discussion, this report presents the results of only two models: (1) the "monthly"[147] estimates are based on the model using four captures of one-week each and the M_{th} model with Chao's lower bound estimator; and (2) the annual estimates are based on the model using 13 captures of four weeks each and the open population estimator.

The study team also experimented with models that included other variables (e.g., Reporting ESP, Source, Victim Age, PhotoDNA, etc.) in the data set as covariates in the model. However, most of the variables had too much missing data or too many categories to create reliable models. Therefore, IP address was the only variable included in the final models.

METHODS FOR THE ANALYSIS OF OPEN TEXT DATA WITHIN CYBERTIPLINE REPORTS

There are three fields within NCMEC CyberTipline reports in which reporters can enter open-ended text to add information related to the report. These fields are not mandatory, so there is varying quality in the data entered in these fields. Some reporters leave these fields blank; others write short, unspecific descriptions (e.g., "inappropriate content shared"); still others include entire chat logs between people associated with reported accounts. To estimate the percent of internet-based CSE that is OSEC, IJM criminal analysts reviewed the open-text data of a sample of CyberTipline reports.

SAMPLING STRATEGY

The initial intention was to pull simple random samples of CyberTipline reports with open-ended text data for each year (2014-2017), so that researchers could combine the data with the annual mark-recapture estimates to calculate the annual number of Philippine-based IP addresses that were associated with suspected OSEC activity. However, the study team determined that, given the available time and resources, they would be unable to review a representative sample of CyberTipline reports from each year in the study period, at the desired

[147] "Monthly" is a term used for simplicity of discussion. However, it relates to a four-week time period, not a calendar month.

95% confidence level. Rather than lowering the confidence level for the sample, the study team decided to pull samples only from years 2015 and 2017 CyberTipline reports. The researchers determined that calculating the number of Philippine-based IP addresses that were associated with suspected OSEC activity for every-other-year in the study period would be enough to establish a general trend and, for IJM's programmatic purposes, would suffice as a baseline measure of prevalence.

To create the sample of CyberTipline reports, NCMEC provided IJM with a list of the CyberTipline Report IDs, Report Date/Time, and IP Addresses of the subset of CyberTipline reports that had at least one entry in one of the open-ended text fields of the report. The end goal of this part of the study was to calculate an annual "percent of internet-based CSE that included suspected OSEC activity" and apply it to the "estimated number of IP addresses used for CSE" that was calculated through the mark-recapture analyses. Thus, CyberTipline reports needed to be sampled by IP address, rather than by Report ID, to ensure that there was a common unit of measure between the two statistics. As a result, an IP address that was reported in multiple CyberTipline reports had the same odds of being sampled as an IP address that was reported in only one CyberTipline report. But a CyberTipline report that reported five IP addresses had a five times higher probability of being sampled than a CyberTipline report that reported only one IP address.

SAMPLE #1

For 2015, there were 10,173 CyberTipline reports with open-ended text, associated with 16,648 unique IP addresses. For 2017, there were 39,243 CyberTipline reports with open-ended text, associated with 56,193 unique IP addresses. To estimate the "percent of internet-based CSE that included suspected OSEC activity" at the 95% confidence level and with 5% margin of error, it was determined that the 2015 sample needed to include 372 unique IP addresses and the 2017 sample needed to include 380 unique IP addresses. The study team chose the final samples using random sampling without replacement.

As noted above, each unique IP address could be reported by multiple CyberTipline reports. Therefore, while the 2015 and 2017 samples included 372 and 380 IP addresses, respectively, they included significantly more CyberTipline reports. In the 2015 sample, each IP address was reported in 1 to 14 CyberTips, and the final sample included a total of 462 unique CyberTipline reports. In the 2017 sample, each IP address was reported in 1 to 25 CyberTipline reports, and the final sample included a total of 606 unique CyberTipline reports.

After the first round of data collection, the primary variable of interest (OSEC Status) was unknown (e.g., the CyberTipline report did not contain enough open-text data to assess OSEC Status without an in-depth investigation) from 874 (82%) of the CyberTipline reports sampled. This prohibited the team from being able to make inferences about the "percent of internet-based CSE that included suspected OSEC activity" at the desired confidence level and margin of error. Therefore, the study team decided to adjust the sampling frame and pull a second full sample of CyberTipline reports from each year.

SAMPLE #2

The study team used the knowledge they had gained from the first round of CyberTipline reviews to adjust the sampling frame for the second round of data collection. Because the majority of CyberTipline reports were auto-referred from ESPs, they often contained "template" language that was repeated in all CyberTipline reports of the same kind. The team identified seven "template" keywords or phrases that were only used in CyberTipline reports that either (1) had a very small amount of text data (such that OSEC Status could not be determined without further investigation) or (2) were unlikely to be associated with OSEC activity (e.g., memes, animated content, or viral content).

The analysts did a file search of all CyberTipline reports with open-ended text to identify the CyberTipline reports that contained each of these "template" phrases. The Report ID for each CyberTipline report containing a "template" phrase was recorded, and the related entry in the sample frame was labeled appropriately. These CyberTipline reports were removed from the sampling frame before the second sample was drawn. Through this process, a total of 10,095 CyberTipline reports were removed from the 2015 sampling frame, and 6,504 CyberTipline reports were removed from the 2017 sampling frame.

Despite the adjustment of the sampling frames, the sample sizes required to obtain results with the desired confidence level and margin of error, did not change. The 2015 sample needed to include 372 unique IP addresses and the 2017 sample needed to include 380 unique IP addresses. Again, the study team chose the second samples using random sampling without replacement. In the 2015 sample, each IP address was reported in 1 to 25 CyberTipline reports, and the final sample included a total of 509 unique CyberTipline reports. In the 2017 sample, each IP address was reported in 1 to 21 CyberTipline reports, and the final sample included a total of 699 unique CyberTipline reports.

Because researchers sampled by IP address rather than CyberTipline Report ID, there were a few CyberTipline reports in the second sample that were also reviewed in the first sample. (These CyberTipline reports all reported multiple IP addresses, and one of the reported IP addresses was randomly selected in the first sample while another was selected in the second sample.) Therefore, the total sample size for each year is slightly smaller than the sum of both sample sizes. The combined 2015 sample included 966 unique CyberTipline reports related to 744 unique IP addresses, and the final 2017 sample included 1,289 unique CyberTipline reports related to 760 unique IP addresses.

DATA COLLECTION

DATA COLLECTION TOOL

IJM's criminal analysts and research experts collaborated to create the data collection tool. The final instrument included six questions to guide the criminal analysts in determining if each CyberTipline report being reviewed was associated with suspected OSEC activity, as well as an open-ended text field for the analysts to write notes about the CyberTipline report. A description of these seven fields is provided in Table 4.

TABLE 4. Data Collection Tool Questions, Answers, and Relevance to OSEC

	Question	Answer Choices	Relevance to OSEC Definition
1	Was there clear evidence that the purpose was online publication?	Yes/No/Maybe	The production, for the purpose of online publication or transmission…
2	Was there clear evidence of sexual abuse or sexual exploitation?	Yes/No/Maybe	… of visual depictions (e.g., photos, videos, live streaming) of the sexual abuse or exploitation…
3	Was there clear evidence that the victim was a minor?	Yes/No/Maybe	… of a minor…
4	Was there clear evidence that the case involved a third-party abuser?	Yes/No/Maybe	… for a third party who is not in the physical presence of the victim…
5	Was there clear evidence of commercial compensation?	Yes/No/Maybe	… in exchange for compensation
6	In your professional opinion, was this a case of OSEC?	Yes/No	This question was included to allow for exclusion of non-OSEC crimes that include the above factors (e.g., sextortion) and inclusion of incidents for which evidence of one of the factors was not *clear* but seemed highly likely, based on the analyst's professional opinion
7	Comments	Open-ended text	Description of incident and explanation of reasoning required for all CyberTipline reports for which Q6 does not seem to align with Q1-5. Description of incident optional for all other CyberTipline reports.

The first five questions in the data collection tool were used to guide the criminal analysts in identifying the elements of suspected OSEC activity in the open-text data. Questions 6-7 allowed the criminal analysts to record their final determination of the CyberTipline's suspected OSEC Status, based on their professional knowledge and experience, and explain their reasoning. This was necessary for two reasons. First, it was possible for a CyberTipline to include all five elements of suspected OSEC activity but not be an instance of OSEC. For example, if criminal analysts reviewed a CyberTipline report related to sextortion (a crime type that includes all five elements of OSEC but is distinct from OSEC), they would answer "Yes" to Questions 1-5 but "No" to Question 6. Second, it was possible for the open-text data to fail to provide "clear" evidence of one of the elements but to provide enough evidence that the criminal analyst suspected that the CyberTipline report was still a probable instance of OSEC. For example, "clear" evidence of commercial compensation was rarely seen because most CyberTipline reports include only the few lines of a chat log (if any) that were written immediately before and after CSAM/CSEM was shared. If compensation was discussed earlier in the chat log, it would be missed in the CyberTipline report. But if all the other elements of the crime were present, a criminal analyst could still determine that the CyberTipline report was associated with suspected OSEC activity.

IJM's data collection team verified the data collection tool by piloting it with 50 CyberTipline reports that were not in the initial sample. The analysts found that many CyberTipline reports did not have any information about the type of activity being reported. (Typically, these CyberTipline reports provided information on the users being reported rather than on the activity they were engaged in.) In these situations, all the questions were inapplicable. Since all the Yes/No questions were mandatory, this made the data collection process overly burdensome. As a result, a question was added to the beginning of the data collection tool (Did this CyberTipline report include information that is useful for identifying the type of crime committed?), and Questions 1-6 were made conditional upon a positive response to the introductory question.

DATA COLLECTION TRAINING AND METHODS

Four of IJM's criminal analysts reviewed the NCMEC CyberTipline reports and recorded the relevant data. These analysts were experienced at analyzing investigative data and were familiar with the elements of OSEC cases. Prior to data collection, they attended a training on the study purpose, methodology, and the data collection tool, including the questions and the online survey platform into which data were entered.

Prior to data collection, NCMEC pulled all the data from the open-ended text fields for all 2015 and 2017 CyberTipline reports with one or more entries in the open-ended text fields. Each field was saved as a separate text file, stored within a folder labeled with the CyberTip Report ID. So, for example, if a CyberTipline report contained entries for all three of the open-ended text fields, the folder for that CyberTip would contain three text files, one for each data field. No other CyberTipline data (e.g.., no data from other fields within the CyberTipline report and no photo or video files) were stored within these folders.

Because open-ended text data has more potential to include personally identifiable information (such as victim or perpetrator names) than a simple list of reported IP addresses, extra data security measures were taken for this portion of the study. All study data were collected within NCMEC's offices. All raw CyberTipline data were stored on flash drives that remained locked up when not in use. The flash drives and files contained within them were never removed from NCMEC's office. The data collection team arranged with NCMEC when to enter the office and collect the data. Upon arriving, the team would check in with NCMEC staff and be given access to the flash drives. They then went to a private, secure space within the office to review the CyberTipline reports and record the relevant study data. Prior to leaving each day, the analysts would return the flash drives to the appropriate NCMEC staff.

DATA HANDLING AND ANALYSIS

The criminal analysts entered CyberTipline data using a laptop, eliminating the need for manual data entry. Collected data were uploaded to an online survey platform via an encrypted connection and then wiped from the criminal analysts' devices. The online survey platform protected submitted data using AES-256 encryption.

To ensure data quality and reliability of CyberTipline coding between analysts, a researcher chose a random sample of 15% of each analysts' CyberTipline reports and assigned them to a different analyst to re-review. Any discrepancies in coding between the original and second analysts were discussed with the entire team of criminal analysts and a joint decision was made on how the CyberTipline should be coded. This data quality assurance process revealed relatively low inter-rater reliability in coding of Questions 1-5. A post-data-collection debrief revealed that the criminal analysts were unclear about the definitions of some terms (e.g., "third-party abuser") that were defined differently in the study than they were in typical investigations, leading to the low inter-rater reliability. However, there was strong agreement on the responses to Question 6 on the analysts' overall professional assessment of the CyberTipline and on the comments provided in Question 7. Thus, it was determined that coding of "OSEC Status" should be conducted based on the responses to Questions 6-7, rather than on the aggregate responses to Questions 1-5.

After all data were collected, researchers downloaded the final database onto their password-protected laptops for cleaning and analysis. The data were stored in an Excel database, and variables were inspected and triangulated to ensure that the data were clean. A single analyst manually reviewed and coded all the notes recorded in Question 7. "OSEC Status" was then coded based on the responses to Question 6 and the coded notes from Question 7. OSEC Status codes are described in Table 5.

TABLE 5. OSEC Status Codes

OSEC Status Code	Description
Not OSEC	CyberTipline reports for which the specific internet-based CSE could be identified, and which was something other than OSEC. These included CyberTipline reports reporting animated images and cases of sextortion/blackmail.
Unlikely OSEC	CyberTipline reports for which the specific internet-based CSE could not be definitively identified, but which seemed unlikely to be a case of OSEC. This included CyberTipline reports related to viral images/memes, sexting between teenagers (no adult involvement) or adults (no child involvement), and chat logs with no references to sexual exploitation/abuse or image sharing.
Possible OSEC	CyberTipline reports for which the specific internet-based CSE could not be definitively identified as OSEC, but which included some elements indicative of OSEC. Most of these included clear evidence of online sexual exploitation of a minor but commercial compensation could not be confirmed. Some cases involved clear solicitation of in-person abuse for exchange of money, but it was unclear if there was an additional online component to the abuse.
OSEC	CyberTipline reports for which there was clear evidence of all elements of suspected OSEC activity.
Unknown	CyberTipline reports for which there was not enough information to make any determination of OSEC status.

ANALYSIS

The study team did not conduct the intended analyses with this data. Even after adjusting the sampling frame and reviewing a second full sample of CyberTipline reports, there was still too much missing data in the primary variable of interest (OSEC Status) for the team to feel confident that the analyses would produce meaningful results. However, the notes provided in Question 7 provided an interesting source of qualitative data. These notes were not mandatory fields within the data collection tool, so they were not consistently entered. However, researchers were able to code the data in these notes to pull out some anecdotal findings from this data collection effort.

ETHICAL CONSIDERATIONS

The study team recognized that there were risks associated with accessing detailed reports of possible child sexual abuse/exploitation. Steps were taken throughout the study to minimize the risk-benefit ratio to those involved in the study, including the people whose data were reported in the CyberTipline reports.

As previously mentioned, several steps were taken to minimize the risk of loss of confidentiality for those whose data were reported in CyberTipline reports. These included (1) collecting all data at the secure office of NCMEC; (2) not recording any personally-identifiable information; and (3) storing and transferring all data in secure ways. To minimize risks to the criminal analysts who reviewed the CyberTipline reports, both NCMEC and IJM provided the analysts with training on self-care and access to self-care resources.

To maximize potential benefit to victims whose data were reported in CyberTipline reports, the criminal analysts were instructed to record CyberTipline report IDs that (1) indicated severe, imminent, and/or ongoing abuse; and (2) contained enough information for law enforcement to investigate. These report IDs were shared with Philippine law enforcement with recommendations to prioritize follow-up on these CyberTipline reports.[148]

Case File Review Methodology

SAMPLING STRATEGY

The primary law enforcement agencies that investigate OSEC cases in the Philippines are the Philippine National Police Women's and Children's Protection Center (PNP WCPC) and the National Bureau of Investigation's Anti-Human Trafficking Division (NBI-AHTRAD). Cases of OSEC were beginning to be identified and investigated in the Philippines during the baseline study period (2010-2017), so PNP WCPC and NBI-AHTRAD had received referrals for and/or investigated fewer than 150 cases. Therefore, the study team decided to review 100% of the cases referred to or investigated by these two law enforcement agencies between January 2010 and December 2017.

DEFINITION AND DESCRIPTION OF CASES

For this study, a "case" was defined as any one of the following:

- A case referred to Philippine law enforcement that had not yet been investigated by Philippine law enforcement;
- A case referred to Philippine law enforcement that had been investigated by Philippine law enforcement; or
- A case proactively generated and investigated by Philippine law enforcement without a referral.

Most case referrals came from international law enforcement agencies, based on information they had obtained while investigating an OSEC customer in their jurisdiction. Due to the nature

[148] Note: NCMEC makes all Philippine-based CyberTipline reports available to Philippine law enforcement, so they already had access to the CyberTipline reports that the criminal analysts flagged for follow-up. However, because Philippine law enforcement receives hundreds of thousands of CyberTipline reports each year, it can be challenging for them to review and triage all the CyberTipline reports. This effort was intended to support the triaging of these CyberTipline reports.

of such investigations, these files typically had more information on the customers and the criminal process used by the customers than on the Philippine-based traffickers or victims.

Philippine investigation case files, on the other hand, were based on information obtained from Philippine law enforcement while investigating a trafficker. Due to the nature of these investigations, these files typically contained little information on the customers but much more detailed information on the victims and traffickers. Most information in these files about the criminal process was related to methods used by traffickers to interact with undercover investigators. Interactions between undercover investigators and traffickers may differ from interactions between actual OSEC customers and traffickers for ethical, legal, and strategic reasons. Therefore, information collected from Philippine investigation case files may not be entirely representative of how actual OSEC customers and traffickers interact.

For cases that had been referred to *and* investigated by Philippine law enforcement, the case referrals and the Philippine investigation case files were matched to create a single record, but the referral and investigation data were kept separate (e.g., data on the offending process found in the referral were recorded separately from data on the offending process found in the investigation case file). This allowed researchers to compare information found in both the case referral and the investigation case file. In particular, researchers were interested in comparing (1) the number and characteristics of victims identified in case referrals vs. investigation case files, and (2) the criminal processes reported in case referrals (detailing interactions between real OSEC customers and traffickers) vs. investigation files (detailing interactions between undercover investigators and OSEC traffickers).

DATA COLLECTION

DATA COLLECTION TOOL

IJM's research, OSEC program, and law enforcement development teams collaborated to create the data collection tool. Europol had conducted a similar case file review study with Western law enforcement agencies the year before IJM designed their tool, and IJM experts used the Europol data collection tool as a starting point for creating the data collection tool for this study. IJM's investigations and law enforcement experts used their knowledge of typical case referrals and Philippine investigation case files to modify the tool and ensure it was contextualized.

The final instrument had three sections and nine sub-sections, with a total of 61 questions. Section A captured information about how the case was initiated and if it had been investigated by Philippine law enforcement. This determined whether one or both of the other two sections would be completed. Section B captured information about the case referral received by Philippine law enforcement. This section was completed only if the case was initiated through a referral from an international law enforcement agency. Section C captured information about the Philippine law enforcement investigation. This section was completed only if an investigation had been conducted and had resulted in an operation, arrest, or victim rescue. (Records on investigations that were started but had not yet led to an operation, arrest, or rescue were usually incomplete, often quite sparse, and had the potential to be inaccurate because the investigation was still in process and information had not all been confirmed. Researchers, therefore, determined that it was best to exclude this data from the study.) Sections B and C both included four sub-sections, capturing information on the typology of (1) the victim/s, (2) the customer/s, (3) the traffickers/s, and (4) the offending process.

Each section and many of the sub-sections were conditional, and many of the sub-sections could be repeated for each victim, customer, or trafficker identified in the case. Therefore, there was large variation in the length of each case file review. The average (mean) time spent on each case file review was around 50 minutes.

IJM's data collection team verified the data collection tool by piloting it with three case files. The enumerator recorded problematic or confusing questions and concerns about the flow of the questions. The study team made changes to the data collection tool based on that feedback, and the enumerators re-reviewed the first three case files and updated the data to ensure they aligned with the new wording of questions. The updated version of the data collection tool was used until about half-way through data collection, when additional changes were made to reduce the data collection burden. This included making some questions conditional based on other questions; deleting questions for which data were consistently missing from case files; adding answer choices for frequently observed responses that had previously been answered as "Other, please specify:"; and adding "Unknown" answer choices for questions that had previously been left blank when the data were missing. The second round of changes to the data collection tool did not require enumerators to re-review any case files. All changes could be made to the data by cleaning and recoding the existing data.

DATA COLLECTION TRAINING AND METHODS

A single enumerator collected the data on all the case files in the study. The enumerator attended a training on the study methodology and the data collection tool, including the questions and the online survey platform into which data were entered.

However, IJM's study team determined that the enumerator should not review case files alone because law enforcement case files are difficult for laypeople to navigate, and because the files contain highly sensitive data, including photographic evidence, that should be shared only on a need-to-know bases. Therefore, at least one experienced IJM OSEC investigator accompanied the enumerator on each case file review. The investigators who accompanied the enumerator had significant experience investigating OSEC crimes and working with Philippine law enforcement, and many had been involved in the investigations they were reviewing, so they were already knowledgeable about where to find information within a case file. Thus, to collect the data, the experienced investigator(s) searched the case files while the trained enumerator asked the investigator questions from the data collection tool and recorded the responses.

Data were collected from two primary sources: Philippine law enforcement case files and IJM case files. IJM has supported almost all OSEC investigations conducted by Philippine law enforcement and helps to provide aftercare to rescued survivors. For program purposes, IJM keeps its own records of cases, which includes data about IJM's involvement in cases but excludes more sensitive data, like CSEM.

To minimize the amount of time (and thus, disruption) spent collecting data at the Philippines law enforcement offices, enumerators first collected data on IJM-supported cases using IJM case files. They then moved to the offices of the Philippines law enforcement agencies that stored the law enforcement case files, where they collected data from case referrals sent to Philippine law enforcement from international law enforcement agencies. Files were never removed from these offices. The data collection team (enumerator and investigator pair) contacted each office to identify convenient times to enter and collect the data. Upon arriving, the team would check in with law enforcement agency office staff and be given access to the case files. They then found a private, secure space within the office to review the case files and record the data.

Researchers successfully collected data on all cases investigated by PNP WCPC or NBI-AHTRAD and on all cases referred to PNP WCPC. However, the team was not able to collect data on OSEC referrals to NBI-AHTRAD that had not led to an operation, rescue, or arrest. OSEC cases at NBI-AHTRAD are not labeled as "OSEC" cases but are given the broader label of "Trafficking" cases. Case data are not stored in a database, and case files are not stored in a single location but are distributed to the investigator in charge of each case. Therefore, there was no way for researchers to sort through "Trafficking" case files to identify and review the OSEC cases, without significantly disrupting the NBI-AHTRAD investigators' work. Thus, the final sample included 100% of OSEC cases referred to PNP WCPC, but only the cases referred to NBI-AHTRAD that had been investigated and resulted in an operation, arrest, or rescue. Table 6 presents the total number of cases reviewed, disaggregated by type of case file (only case referral, only a Philippines investigation, or both a case referral and a Philippines investigation).[149]

TABLE 6. Case File Review Sample

	Total
Total Case Files Reviewed	**92**
Case Referral Only	21
PHI Investigation Only	28
Case Referral + PHI Investigation	43

DATA HANDLING AND ANALYSIS

The enumerator collected case file data using a laptop, and the data were uploaded to the same online survey platform tool described in the "Methods for the Analysis of Open Text Data within CyberTipline Reports, Data Handling and Analysis" section. When not in use, the laptop was logged out of the online survey platform and stored inside the secured IJM Philippines National Office.

A researcher quality-checked more than 15% of case files to ensure that all questions were answered and that answers followed logical patterns (e.g., if the data showed that four victims were identified in a case file, then the enumerator should have entered demographic data for four victims). A 100% sample of the first three case files were quality-checked before the enumerator was permitted to continue data collection. Thereafter, the researcher quality-checked a random 15% sample of newly collected case file reviews each week. All missing data and inconsistent patterns were immediately shared with the enumerator, and he was asked to provide an explanation for the inconsistencies or re-review the case file to find the missing data. If minor errors (e.g., leaving a question blank instead of answering "Unknown") were found in

[149] Note: There is a discrepancy between the number of cases referred to the Philippines as reported by international law enforcement data and Philippine law enforcement case data. Possible explanations for these discrepancies include: (1) For this study, researchers only looked at cases reported to PNP and NBI—the law enforcement agencies within the Philippines that most often investigate OSEC cases. However, international law enforcement agencies may have referred cases to other Philippine law enforcement agencies, and the cases may not have been transferred to PNP or NBI. (2) Philippine law enforcement may label cases differently than international law enforcement does. For example, if multiple international case referrals pointed to the same Philippine trafficker, Philippine law enforcement may have combined the referrals into a single case file. (3) Each international law enforcement agency uses a slightly different definition of OSEC. It may be that some cases labeled as "OSEC" by international law enforcement agencies were labeled as a different crime by Philippine law enforcement and thus were not counted in their case files.

the same question across multiple case files, then clarifications on the desired responses were given to the enumerator for future case file reviews, and a note was made for the data analyst to check for similar errors in other records during data cleaning. No major errors were found through the data quality checks, and the enumerator was able to explain most inconsistent patterns by unusual circumstances in the case.

After all data were collected, researchers downloaded the final database onto their password-protected laptops for cleaning and analysis. The data were stored in an Excel database, and variables were inspected and triangulated to ensure that the data were clean. Recoding and data analysis were conducted using Excel.

LIMITATIONS

Researchers intended to collect data on all OSEC cases referred to or investigated by PNP WCPC or NBI-AHTRAD between 2010 and 2017. However, due to the previously discussed data collection challenges, the team was not able to collect data on any OSEC cases referred to NBI-AHTRAD OSEC that had not resulted in an operation, arrest, or rescue. The team was unable to determine how many such cases exist. Therefore, the final sample included 100% of PNP WCPC's OSEC case files (investigations and referrals) and a nonrandom sample of an unknown percent of NBI-AHTRAD's OSEC case files (investigations only). However, researchers have no reason to believe that the missing cases represent a particularly large proportion of all cases, or that the non-investigated NBI-AHTRAD OSEC cases differ significantly from investigated NBI-AHTRAD OSEC cases. Thus, the study team does not think that the inability to collect this data undermines the representativeness of the results.

It is also worth mentioning that, while the researchers believe that the results of this portion of the study are representative of OSEC cases that have been referred to or investigated by Philippine anti-trafficking units, it is not necessarily representative of all *incidents* of OSEC. There may be some characteristics of the studied cases (including characteristics of the victims, customers, traffickers, or offending processes) that make them more likely to be investigated than other instances of OSEC. For example, some countries' law enforcement agencies are more proactive and efficient at, and/or have more resources allocated to, investigating OSEC customers in their own countries and sharing relevant evidence with Philippine law enforcement. Naturally, the study showed that most customers are from these countries, even though there may be many customers from other countries that put fewer resources into investigating these crimes and thus remain uncaught. Therefore, this research is skewed towards the processes and people that are more likely to be detected. Similarly, for the study period (2010-2017), Philippine law enforcement did not have equal capacity to investigate OSEC cases in all areas of the country, so the geographic distribution of cases was as much a function of law enforcement capacity as actual OSEC incidence.

Appendix B. Alternate Methodologies Considered

Prior to designing this study, the study team spent years exploring potential methodologies and sources of data for determining the prevalence of OSEC in the Philippines. In hopes that others may learn from our process and in recognition that others may be able to build on our rejected ideas, the eight methodologies *not* selected for this study are presented here.

SURVEY OSEC "HOT SPOTS"

First, the study team considered the use of randomized surveys in known OSEC "hot spots," as identified through Philippine law enforcement case work, to measure the prevalence of OSEC. To do this, the study team could use a survey system modeled on the Youth Risk Behavior Surveillance System (YRBSS),[150] which was developed by the Center for Disease Control (CDC) and has been used successfully for several years in the United States. This method was ultimately rejected based on the following five challenges.

Challenges:

- *Accuracy of Data:* Questions regarding sexual exploitation are obviously quite sensitive, and OSEC survivors would be naturally hesitant to answer honestly.
- *Ethical Concerns:* Based on IJM's casework, victims of OSEC are often incredibly young (often below the age of 10), and it would be unethical to try to conduct a broad survey with children in the age range of our clients, asking about their sexual exploitation experiences.
- *Data Delays:* To avoid surveying children, the team could survey adults to measure *historic* OSEC prevalence in the survey area. This would result in a 10- to 14-year lag in OSEC prevalence because respondents would be answering questions about events that happened in their childhood.
- *Resource Limitations:* Due to resource considerations, the survey area assessed would have to be a small subset of IJM's OSEC project area (which includes all of the Philippines). Thus, the team would lack any data on the potential displacement of OSEC to other areas as a result of increased law enforcement action in the "hot spot."
- *Accuracy of "Hot Spots":* Unlike traditional forms of child sex trafficking, which naturally occur in highly urban areas in order to maximize access to potential customers, OSEC can flourish anywhere that internet access is available. The only data we have to determine where "hot spots" may be is Philippine law enforcement case data. However, law enforcement cases represent a small fraction of the actual problem and may not be representative of all OSEC occurrences.

UNDERCOVER INVESTIGATIONS

IJM's Philippines offices have previously used undercover investigation work to determine the prevalence of location-based commercial sexual exploitation of children. Therefore, the study team considered a similar approach for measuring OSEC prevalence. The idea was to work with local law enforcement to record interactions with suspected OSEC traffickers in the Philippines using undercover (U/C) accounts on social media. This approach could include a passive or proactive approach. A passive approach would include IJM and its law enforcement partners waiting for potential OSEC traffickers to contact one of the fake U/C profiles, while a proactive

[150] Division of Adolescent and School Health, National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention. (2018). Youth Risk Behavior Surveillance System. Retrieved from: https://www.cdc.gov/healthyyouth/data/yrbs/index.htm

approach would include proactively befriending and engaging accounts which fit a particular profile for a Filipino trafficker.

The study team also explored the possibility of working with external experts to build a social media "chatbot" that is capable of independently engaging in basic conversation with potential OSEC traffickers in the Philippines. If specific keywords were identified in the conversation, then we could record this as a potential "hit" for the purposes of tracking prevalence, while also turning over the chat logs to IJM's investigation teams and law enforcement for follow-up. This method was ultimately rejected based on the following four challenges:

Challenges:

- *Few Results and False Positives*: A passive approach in which IJM and its law enforcement partners waits for potential OSEC producers to contact one of the fake U/C profiles was not a viable approach because, based on IJM's experience, this would produce a very low number of potential contacts and insufficient basis to determine whether the individual may be engaged in OSEC.
- *Lack of Technical Capacity:* There is a high technological burden in creating a "chatbot" sophisticated enough to engage potential OSEC producers in conversations that are sufficiently complex in order to determine whether the individual may be an OSEC trafficker.
- *Ethical/Legal Concerns:* There were concerns over the possibility that during any sort of passive or proactive engagement, the OSEC traffickers could unexpectedly and without solicitation send child abuse material to one of the study's undercover investigators. This would result in the study team possessing contraband material and possible evidence of new abuse or exploitation of children.
- *Accuracy of Data over Time:* There is no way to extrapolate the findings from this type of study to the general population to get a prevalence rate. It can only provide the number of "hits" of OSEC identified in a certain time frame, and that number is likely to be impacted by many factors (e.g., investigative techniques) other than background prevalence of the crime. IJM wants to be able to replicate this methodology at the end of the project period, and as these other factors change, IJM's ability to compare the results of the baseline and endline studies to draw conclusions about the prevalence of OSEC would be compromised.

DARK WEB CONTENT SCRAPING

One of the first data collection methodologies IJM explored was to scrape content from pedophile message boards hosted on the dark web. In late 2014, there was a system that stripped out all child abuse material and images from the boards prior to transmission, which allowed a user to scrape the content without ever being in possession of illegal material. IJM explored using such a system to scrape the conversations from these boards and search them for keywords potentially indicating the production and distribution of child pornography in the Philippines. This method was ultimately rejected based on the following two challenges:

Challenges:

- *Failure to Align with Definition of OSEC:* These web forums hosted on the dark web are places where foreign pedophiles (those outside the Philippines) trade images and videos. There is no indication that these web forums serve as a connection point between child pornography producers in the Philippines and foreign pedophiles. IJM concluded that even if it was able to scrape these web forms for content and analyze the data, it was

unlikely to produce any usable information regarding the prevalence of OSEC in the Philippines, as defined by IJM's programs.
- *Lack of Access:* The pedophile-oriented web forums on the dark web became significantly more difficult (and in many cases impossible) to access in early 2015. This eliminated the dark web as a viable source of information to measure OSEC prevalence and Philippines.

DATA FROM MONEY TRANSFER AGENCIES (MTAs)

In early 2015, IJM explored the possibility of estimating prevalence based on data from money transfer agencies (MTAs) in the Philippines. After conversations with representatives of various MTAs, IJM learned that some agencies attempt to track transfers that fit a pattern that could be OSEC. This method was ultimately rejected based on the following challenge:

Challenges:
- *Lack of Specificity/Reliability:* The MTAs noted that while the pattern they track may indicate that a transfer is related to OSEC, there are a number of other non-criminal scenarios that also fit this pattern. Consequently, *even if* IJM were to gain access to such information from multiple MTA companies in the Philippines, this is not a reliable measure to estimate OSEC prevalence.

SOCIAL MEDIA NETWORK ANALYSIS

IJM explored a few options to gather OSEC prevalence data from various social media platforms. The study team focused on social media because IJM investigators have observed that social media platforms are some of the most common connection points between OSEC traffickers in the Philippines and customers located abroad.

One approach the study team explored was to build a model of the typical attributes of a social media profile for individuals known to be involved in the production of child abuse material in the Philippines based upon IJM's existing OSEC casework experience. Given an accurate model of the typical OSEC trafficker in the Philippines, the team theorized that it might be possible to ask key social media platforms to scan their existing user bases and record the number of profiles that matched the attributes of our model profile. This method was ultimately rejected based on the following challenges:

Challenges:
- *Ethical Concerns:* User privacy/data protection is a growing concern in social media. This idea was considered years before the most recent debates began over the way social media sites use user data. But even then, this was a significant concern that impeded IJM's interest in pursuing this methodology.
- *Lack of Specificity/Reliability:* Even if IJM was able to construct a model profile that accurately describes the key attributes of typical OSEC traffickers in the Philippines, there would be no way of knowing whether this model also produced false positive matches for individuals who were not engaged in OSEC.
- *Lack of Technical Capacity:* IJM discussed this approach with contacts at some social media sites. They reported that even if the company was willing to disclose such information to IJM (which seemed unlikely given the aforementioned user data

protection concerns), they also indicated that the companies do not have the technical capability to scan their profiles with the level of granularity needed for such an approach.

ETHNIC ANALYSIS OF NEW CHILD SEXUAL ABUSE MATERIALS

IJM explored with NCMEC the possibility of conducting analysis of the ethnicity of victims and suspects depicted in newly identified child sexual abuse materials (CSAM). If possible, this might allow the study team to record the percentage of victims in newly identified CSAM who are of Filipino origin and, over time, estimate whether the volume of production of CSAM originating in the Philippines is increasing or decrease. While this approach initially appeared to be promising because NCMEC maintains a comprehensive database of all identified CSAM, the method was ultimately rejected based on the following three challenges:

Challenges:

- *Inconsistency in Quality of Data:* Project Vic maintains the database of identified CSAM. Law enforcement officers around the world can access the Project Vic database and update information on identified images and victims, including suspected ethnicity. However, it is not mandatory for international law enforcement to update this information, and they often do not. As a result, a high percentage of CSAM in the Project Vic database does not include any information regarding the ethnicity of victims.
- *Lack of Technical Capacity:* IJM explored whether the missing data issue could be overcome through a facial recognition software system that is capable of identifying the ethnicity of victims in Project Vic's database. Unfortunately, to the study team's knowledge, no form of ethnic recognition software exists.
- *Failure to Align with Definition of OSEC:* The biggest challenge with this approach was that it could not determine whether newly identified CSAM represented new/ongoing abuse or depicted abuse that was only recently identified but which had happened in the past. Nor would it be clear if the CSAM was exchanged for money, which, by IJM's definition, was a critical component that separated OSEC from other types of child sexual exploitation.

CHILD BEHAVIOR ANALYSIS

IJM briefly considered training adults, who are in regular contact with children (e.g., school counsellors, teachers, youth pastors, etc.), to observe and report child behavior that may have been indicative of abuse. These reports could be categorized as "suspected" or "confirmed," and sorted by the type of abuse (neglect, physical abuse, sexual abuse, online exploitation, etc.). Based on the number of observers and observations of OSEC in each school (or other group of children), the study team may have then been able to estimate the prevalence of OSEC in the surrounding neighborhood. This method was ultimately rejected based on the following challenges:

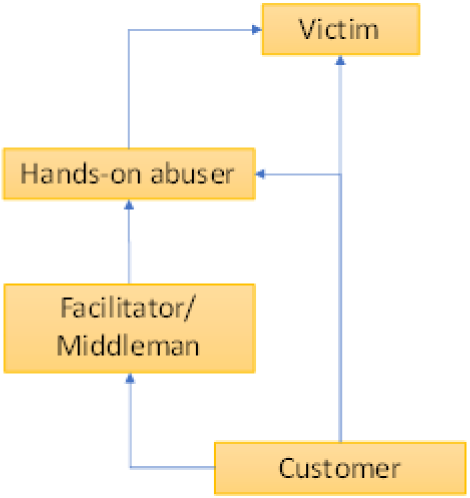
Challenges:

- *False Positives and False Negatives:* Behavioral analysis is not an exact science, and it would be difficult, if not impossible, to train lay observers to consistently and accurately identify children who were displaying symptoms of abuse. Furthermore, there was likely a significant amount of overlap between the symptoms of the various types of abuse and neglect, making it difficult to accurately determine the number of OSEC victims (vs. other types of abuse).

- *Lack of Access to Children and Observers:* IJM did not have access to schools or other groups of children and their normal adult contacts, nor did they have buy-in from such a group to engage in this sort of study. Even if IJM could have gotten access to a group of school-aged children, the study may have missed a significant population of possible victims because, based on IJM's casework, victims of OSEC are often younger than school-age.
- *Legal and Ethical Challenges:* There would be significant ethical and possible legal concerns in having a group of adults identify children as possible victims of abuse. (How can the study team be sure the trained adults were safe and would keep abuse information private and confidential? Did the Philippines have reporting requirements for adults who discover child abuse? Etc.)

MARKET-BASED APPROACH

IJM considered studying the dynamics of OSEC as a marketplace. There were four core categories of actors in the OSEC market (three types of perpetrators and a victim), who interacted with each other like this:



Based on that model, one could attempt to use traditional (or modified) market sizing methods to measure the supply and demand of OSEC. For example, in the IT space, companies like Gartner and Forrester routinely report on the current and predicted future value of new technologies. This method was ultimately rejected based on the following challenges:

Challenges:

- *Proxy Measure of Prevalence:* This method would measure the relative ease of finding a victim or customer, rather than the prevalence or number of incidents of OSEC. For IJM, this kind of proxy measure for prevalence was not considered sufficient for assessing the collective impact of its program.
- *Lack of Expertise:* The study team lacked the necessary expertise to even assess the viability of this method.
- *Replicability:* Not knowing much about this method, it was unclear whether changes in the nature of OSEC (e.g., displacement of the crime from social media to the dark web) would affect the replicability of this methodology at program endline.

Appendix C. Characteristics of NCMEC CyberTipline Data by Year

This appendix provides descriptive statistics on the IP addresses reported to NCMEC between 2014 and 2017. Data are broken down into 13 four-week capture periods. These data were used in the mark-recapture analyses to estimate the annual number of IP addresses used for CSE.

As discussed in Appendix A, the annual estimates were calculated by creating lists of all IP addresses associated with a CyberTipline report during a given four-week period. Groups of 13 consecutive four-week periods (e.g., years) were compared to determine how many IP addresses were reported in more than one four-week period.

Table 7 shows the number of four-week periods in which IP addresses were reported during each year in the study period. For example, we can see from the 2017 column that 35,007 IP addresses were reported in only one four-week period; 5,210 IP addresses were reported in two four-week periods; 1,998 IP addresses were reported in three four-week periods; etc. It should be noted that in this model, if an IP address was reported two or more times within a single four-week period, it would only be counted once. Therefore, the number of four-week periods in which an IP address was reported is not necessarily the same as the number of times an IP address was reported.

TABLE 7. Number of 4-Week Periods in Which Unique IP Addresses Were Captured, by Year

# of Periods	2014	2015	2016	2017
1	9,002	13,909	20,540	35,007
2	670	1,117	2,045	5,210
3	348	515	1,023	1,998
4	206	377	906	1,324
5	162	206	864	904
6	104	133	631	576
7	46	81	430	335
8	17	51	215	190
9	5	24	110	87
10	1	22	48	48
11	1	2	23	30
12	1	2	17	15
13	1	1	13	4
Total	10,564	16,440	26,865	45,728

Tables 8-11 provide more detailed information on the number of IP addresses reported in each four-week time period. Rather than looking only at the *number* of four-week periods IP addresses were reported in, these tables show *which* four-week time period the IP addresses were reported in. The table shows how many IP addresses were reported ("captured") in each time period, the number of IP addresses that were captured for the first time that year in that time period, and the number of IP addresses that were captured for the last time in that time period.

For example, we can see from the first row in Table 8 that 374 IP addresses were reported in the first four weeks of 2014. Since this was the beginning of the year, all of the reported IP addresses were being reported for the first time. But only 240 of the 374 IP addresses were reported for the last time in Weeks 1-4 of 2014. That means that a little over one-third of the IP addresses reported in Weeks 1-4 of 2014 were reported again later in the year.

Table 8. Number of IP Addresses Captured (Captured), Captured for the First Time (First), and Captured for the Last Time (Last) in Each 4-Week Capture Period, 2014

	Captured	First		Last	
		#	(%)	#	(%)
Capture 1 (Week 1-4)	374	374	(100%)	240	(64%)
Capture 2 (Week 5-8)	1,344	1,298	(97%)	825	(61%)
Capture 3 (Week 9-12)	1,403	1,141	(81%)	806	(57%)
Capture 4 (Week 13-16)	1,421	1,015	(71%)	834	(59%)
Capture 5 (Week 17-20)	1,738	1,188	(68%)	1,225	(70%)
Capture 6 (Week 21-24)	418	297	(71%)	298	(71%)
Capture 7 (Week 25-28)	318	202	(64%)	207	(65%)
Capture 8 (Week 29-32)	353	227	(64%)	216	(61%)
Capture 9 (Week 33-36)	1,459	1,042	(71%)	1,069	(73%)
Capture 10 (Week 37-40)	597	419	(70%)	453	(76%)
Capture 11 (Week 41-44)	3,018	2,271	(75%)	2,720	(90%)
Capture 12 (Week 45-48)	557	343	(62%)	478	(86%)
Capture 13 (Week 49-52)	1,193	747	(63%)	1,193	(100%)

Table 9. Number of IP Addresses Captured (Captured), Captured for the First Time (First), and Captured for the Last Time (Last) in Each 4-Week Capture Period, 2015

	Captured	First		Last	
		#	(%)	#	(%)
Capture 1 (Week 1-4)	1,688	1,688	(100%)	891	(53%)
Capture 2 (Week 5-8)	752	642	(85%)	445	(59%)
Capture 3 (Week 9-12)	1,423	1,195	(84%)	942	(66%)
Capture 4 (Week 13-16)	1,249	936	(75%)	766	(61%)
Capture 5 (Week 17-20)	1,343	1,020	(76%)	987	(73%)
Capture 6 (Week 21-24)	1,898	1,261	(66%)	1,053	(55%)
Capture 7 (Week 25-28)	2,124	1,509	(71%)	1,491	(70%)
Capture 8 (Week 29-32)	1,913	1,490	(78%)	1,484	(78%)
Capture 9 (Week 33-36)	1,503	949	(63%)	1,023	(68%)
Capture 10 (Week 37-40)	2,349	1,649	(70%)	1,729	(74%)
Capture 11 (Week 41-44)	4,218	3,260	(77%)	3,755	(89%)
Capture 12 (Week 45-48)	1,325	441	(33%)	1,165	(88%)
Capture 13 (Week 49-52)	709	400	(56%)	709	(100%)

TABLE 10. Number of IP Addresses Captured (Captured), Captured for the First Time (First), and Captured for the Last Time (Last) in Each 4-Week Capture Period, 2016

	Captured	First		Last	
		#	(%)	#	(%)
Capture 1 (Week 1-4)	1,647	1,647	(100%)	899	(55%)
Capture 2 (Week 5-8)	2,497	2,284	(91%)	956	(38%)
Capture 3 (Week 9-12)	2,360	1,789	(76%)	976	(41%)
Capture 4 (Week 13-16)	2,595	1,908	(74%)	1,212	(47%)
Capture 5 (Week 17-20)	2,841	1,839	(65%)	1,574	(55%)
Capture 6 (Week 21-24)	1,337	809	(61%)	546	(41%)
Capture 7 (Week 25-28)	1,818	1,105	(61%)	815	(45%)
Capture 8 (Week 29-32)	2,224	1,279	(58%)	1,057	(48%)
Capture 9 (Week 33-36)	7,469	4,580	(61%)	4,085	(55%)
Capture 10 (Week 37-40)	6,765	3,392	(50%)	3,632	(54%)
Capture 11 (Week 41-44)	6,536	3,040	(47%)	4,008	(61%)
Capture 12 (Week 45-48)	5,628	2,258	(40%)	4,567	(81%)
Capture 13 (Week 49-52)	2,538	935	(37%)	2,538	(100%)

TABLE 11. Number of IP Addresses Captured (Captured), Captured for the First Time (First), and Captured for the Last Time (Last) in Each 4-Week Capture Period, 2017

	Captured	First		Last	
		#	(%)	#	(%)
Capture 1 (Week 1-4)	2,751	2,751	(100%)	1,313	(48%)
Capture 2 (Week 5-8)	4,967	4,737	(95%)	2,782	(56%)
Capture 3 (Week 9-12)	5,093	4,293	(84%)	2,875	(56%)
Capture 4 (Week 13-16)	5,828	4,550	(78%)	3,616	(62%)
Capture 5 (Week 17-20)	5,200	3,840	(74%)	3,498	(67%)
Capture 6 (Week 21-24)	6,652	4,826	(73%)	3,370	(51%)
Capture 7 (Week 25-28)	2,397	1,284	(54%)	1,070	(45%)
Capture 8 (Week 29-32)	2,753	1,208	(44%)	1,189	(43%)
Capture 9 (Week 33-36)	4,919	2,350	(48%)	2,390	(49%)
Capture 10 (Week 37-40)	5,881	2,863	(49%)	3,385	(58%)
Capture 11 (Week 41-44)	5,038	2,252	(45%)	3,179	(63%)
Capture 12 (Week 45-48)	11,440	6,740	(59%)	9,597	(84%)
Capture 13 (Week 49-52)	7,464	4,034	(54%)	7,464	(100%)

Appendix D. Mark-Recapture Estimates of Number of IP Addresses Used for CSE

This appendix provides estimates on the number of IP addresses used for CSE for every four-week and one-year period between 2014 and 2017. These estimates are the result of the mark-recapture analysis of NCMEC CyberTipline reports involving an IP address resolving to the Philippines. The data in these tables correspond to Figures 5 and 6 in the report. However, Figures 5 and 6 plot estimates for overlapping periods (e.g., Jan. 1, 2014-Dec. 31, 2014, Jan. 2, 2014-Jan. 1, 2015, etc.), but for simplicity, we present only the non-overlapping time periods here.

Table 12 provides estimates and 95% confidence intervals for the number of IP addresses used for CSE for every four-week period. These data correspond to Figure 5 in the report.

TABLE 12. Estimated Number (and 95% Confidence Interval) of Philippine IP Addresses Used for CSE in Each Four-Week Time Period, 2014-2017

Time Period	Estimated # of IP Addresses	95% Confidence Interval	
		Lower	Upper
1/6/14-2/2/14	2,723	1,516	3,930
2/3/14-3/2/14	3,087	1,842	4,333
3/3/14-3/30/14	3,643	1,344	5,942
3/31/14-4/27/14	5,521	2,017	9,025
4/28/14-5/25/14	8,403	6,675	10,130
5/26/14-6/22/14	17,765	0	37,684
6/23/14-7/20/14	13,672	11,804	15,541
7/21/14-8/17/14	4,738	2,567	6,910
8/18/14-9/14/14	8,955	7,023	10,888
9/15/14-10/12/14	7,106	5,765	8,447
10/13/14-11/9/14	5,950	5,047	6,853
11/10/14-12/7/14	5,073	4,379	5,768
12/8/14-1/4/15	6,800	5,745	7,855
1/5/15-2/1/15	6,319	5,434	7,205
2/2/15-3/1/15	6,122	5,353	6,890
3/2/15-3/29/15	8,282	6,511	10,054
3/30/15-4/26/15	6,325	4,739	7,911
4/27/15-5/24/15	7,220	5,711	8,729
5/25/15-6/21/15	4,247	3,558	4,935
6/22/15-7/19/15	9,707	8,435	10,978
7/20/15-8/16/15	3,029	2,671	3,388
8/17/15-9/13/15	2,634	1,981	3,287
9/14/15-10/11/15	6,323	4,306	8,340
10/12/15-11/8/15	6,635	5,464	7,805
11/9/15-12/6/15	6,256	4,959	7,554
12/7/15-1/3/16	8,870	6,667	11,074
1/4/16-1/31/16	6,537	5,411	7,663
2/1/16-2/28/16	5,270	4,386	6,154
2/29/16-3/27/16	7,162	6,163	8,160
3/28/16-4/24/16	9,338	8,055	10,622
4/25/16-5/22/16	15,154	14,507	15,801
5/23/16-6/19/16	13,030	12,468	13,592
6/20/16-7/17/16	13,440	12,829	14,051
7/18/16-8/14/16	12,967	12,283	13,651
8/15/16-9/11/16	10,372	8,966	11,778
9/12/16-10/9/16	11,870	10,266	13,474
10/10/16-11/6/16	10,234	8,876	11,591
11/7/16-12/4/16	11,367	9,948	12,786
12/5/16-1/1/17	5,702	5,362	6,042
1/2/17-1/29/17	16,163	13,614	18,712
1/30/17-2/26/17	20,458	19,113	21,802
2/27/17-3/26/17	13,277	11,297	15,257
3/27/17-4/23/17	12,635	11,061	14,209
4/24/17-5/21/17	13,703	12,768	14,638
5/22/17-6/18/17	16,765	15,717	17,814
6/19/17-7/16/16	13,497	12,891	14,103
7/17/17-8/13/17	40,598	38,517	42,680
8/14/17-9/10/17	30,751	28,570	32,932
9/11/17-10/8/17	31,338	27,797	34,880
10/9/17-11/5/17	33,230	29,491	36,969
11/6/17-12/3/17	30,845	28,004	33,686
12/4/17-12/31/17	37,735	33,318	42,151

Table 13 provides estimates and 95% confidence intervals for the number of IP addresses used for CSE for every one-year period. These data correspond to Figure 6 in the report.

TABLE 13. Estimated Number (and 95% Confidence Interval) of Philippine IP Addresses Used for CSE in Each One-Year Time Period, 2014-2017

Time Period	Estimated # of IP Addresses	95% Confidence Interval	
		Lower	Upper
1/1/14-12/31/14	23,333	22,314	24,352
4/1/14-3/31/15	26,719	25,825	27,613
7/1/14-6/30/15	23,146	22,086	24,206
10/1/14-9/30/15	22,617	21,972	23,261
1/1/15-12/31/15	22,708	22,082	23,335
4/1/15-3/31/16	24,621	23,682	25,561
7/1/15-6/30/16	31,606	30,758	32,453
10/1/15-9/30/16	31,956	31,522	32,391
1/1/16-12/31/16	36,144	35,671	36,618
4/1/16-3/31/17	43,658	42,999	44,317
7/1/16-6/30/17	38,659	38,066	39,251
10/1/16-9/30/17	64,883	63,899	65,867
1/1/17-12/31/17	81,723	80,188	83,259