Confronting New Challenges in the Fight Against Child Pornography:

Best Practices to Help File Hosting and File Sharing Companies Fight the Distribution of Child Sexual Exploitation Content

September 2013

A publication of the Asia Pacific Financial Coalition Against Child Pornography, an initiative of the

International Centre
FOR MISSING & EXPLOITED CHILDREN

TABLE OF CONTENTS

ACKNOWLEDGMENTS

The Asia Pacific Financial Coalition Against Child Pornography (APAC-FCACP) wishes to thank the following organizations and individuals for their contributions to this paper:

- Cory Louie of Dropbox
- Jeff Wu of Facebook
- Kenny Logan of PayPal
- Andras Bedoe of RapidShare
- Myla Pilao and Alma Alvarez of Trend Micro, and
- Holly Sais of Veri-Site

The International Centre for Missing & Exploited Children (ICMEC) and the APAC-FCACP gratefully acknowledge the support of PayPal in the development of this Best Practices paper.

DISCLAIMER

This report ("Report") was created and written by volunteers on behalf of the APAC-FCACP and represents the current views of the issues addressed as of the date of publication. The content of the Report is based on the individual input of the contributors, and does not necessarily reflect the opinions or policies of the companies at which the individuals work, nor of any of the APAC-FCACP member companies. There may be inaccuracies or information that has become outdated since this Report was originally written.

This Report is for reference only and does not purport to provide specific legal, financial, or business advice. If you require specific advice or counsel, you should consult with a proper professional. THE APAC-FCACP MAKES NO WARRANTIES, EXPRESSED, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS REPORT. The listing of an organization or entity herein does not imply any sort of endorsement by such organization or entity.

INTRODUCTION

The Financial Coalition Against Child Pornography (FCACP) was formed in 2006 to address the alarming growth of commercial child pornography over the Internet. Its members include leaders in the banking and payment industries, as well as technology companies. The FCACP is managed by the International Centre for Missing & Exploited Children (ICMEC) and its sister agency, the National Center for Missing & Exploited Children (NCMEC).

The Internet has enabled access to child pornography by thousands and possibly millions of individuals around the world. Consumers are able to use traditional payment tools, such as credit cards, as well as new, alternative payment schemes, to purchase child pornography on the Internet. The mission of the FCACP is to follow the flow of funds and shut down the payments accounts used by these illicit enterprises. The situation with commercial child pornography has changed dramatically since the FCACP became operational in 2006. For example, there has been a 50% drop in the number of unique commercial child pornography websites reported into the U.S. CyberTipline, a hotline operated by NCMEC.

The Asia Pacific Financial Coalition Against Child Pornography (APAC-FCACP) was established in 2009 to replicate the efforts of the U.S. Coalition in the Asia Pacific region. It is managed by the Asia Pacific office of ICMEC based in Singapore, bringing together banks, credits card companies, online third-party payment systems, technology companies, social networking platforms, industry associations and law enforcement agencies. Recognizing the important role of civil society and governments in protecting children from online child pornography, the APAC-FCACP urges industry to also recognize responsibility in the online safety sphere and to proactively make efforts to combat this crime and safeguard children.

New business models on the Internet present new challenges in the fight against the dissemination of child pornography. It is the APAC-FCACP's mission to reach out to these new industry sectors to offer guidance on how to avoid being abused by individuals or enterprises who want to use their platforms or services for the distribution of child sexual exploitation images. This document is designed to address the needs of the file hosting and sharing industry.

In its 2011 Trends Report, the Internet Watch Foundation (IWF) noted that over the two previous years it had seen an increasing number of legitimate websites being criminally exploited to host child sexual abuse content. The IWF also reported that image hosting sites (also known as weblockers, cyberlockers or one-click hosting) are the most likely to be abused, with 45% of the reported child sexual abuse content found on those types of sites.

STAYING AHEAD OF THE PROBLEM

File sharing companies are encouraged to take the following precautions to help ensure that child sexual exploitation content is not stored, hosted, reproduced or distributed by users of their services.

Terms and Conditions or Policies

The company's User Agreement should clearly state that any user or account offering illegal content and/or services violates the company's Terms and Conditions or Policies and will be subject to immediate enforcement action and disclosure to appropriate law enforcement authorities and/or the relevant reporting/hotline process. Here are several examples of "acceptable use" policy language:

AT&T Acceptable Use Policy (http://www.corp.att.com/aup)

Child Pornography: IP Services shall not be used to publish, submit/receive, upload/download, post, use, copy or otherwise produce, transmit, distribute or store child pornography. Suspected violations of this prohibition may be reported to AT&T at the following e-mail address: cp@abuse-att.net. AT&T will report any discovered violation of this prohibition to the National Center for Missing and Exploited Children and take steps to remove child pornography (or otherwise block access to the content determined to contain child pornography) from its servers.

Facebook's Community Standards (https://www.facebook.com/communitystandards)

To balance the needs and interests of a global population, Facebook protects expression that meets the community standards outlined on this page. Please review these standards. They will help you understand what type of expression is acceptable, and what type of content may be reported and removed.

- *Facebook has a strict policy against the sharing of pornographic content and any explicitly sexual content where a minor is involved. We also impose limitations on the display of nudity*. (this is one of 10 items on Facebook's list).

Sprint Acceptable Use Policy (http://www.sprint.com/legal/agreement.html)

You may access and use our Website and Network only for lawful purposes. You are responsible for any transmission you send, receive, post, access, or store via our Network, including the content of any communication. Transmitting, distributing, or storing any material that violates any applicable law is prohibited. Additionally, the following non-exhaustive list details the kinds of illegal or harmful conduct that is prohibited.

- *Offensive Materials: Disseminating or posting material that is unlawful, libelous, defamatory, obscene, indecent, lewd, harassing, threatening, harmful, invasive of privacy or publicity rights, abusive, inflammatory, or otherwise objectionable. Without limiting the foregoing, you may not access or use our Website or Network in any manner for the transmission or dissemination of images containing child pornography.* (this is one of 8 items on Sprint's list).

Content Recognition, Filtering or Review
The company should have a formal policy and procedure for reviewing abuse reports of potential child sexual exploitation content. Content confirmed as child sexual exploitation material that is publicly shared should be flagged and further banned from being publicly shared through the company's platform or service. Depending on the company's Terms and Conditions or Policies, known child sexual exploitation content should be prohibited from a company's storage, hosting and sharing features.

Reporting Process
Companies should establish processes to manage receiving abuse reports of users of their service storing, hosting or sharing suspected child sexual exploitation content. A process should be implemented to investigate these types of reports and collect, preserve and report relevant information through the appropriate channel based on applicable laws or process for the location of the company. At the end of this paper, there are descriptions of reporting mechanisms in several countries.

Law Enforcement Response
The company should comply with all applicable laws based on the jurisdiction where the company is located, the location of data, or the location of users. The company should review and respond when applicable to all valid law enforcement requests, including subpoenas, digital evidence requests, search warrants, court orders and other legal process. The company is encouraged to share with law enforcement its legal compliance process, procedures, guidelines and contact information.

User Flagging
Thorn, a group fighting child sexual exploitation, developed a "Sound Practices Guide to Fight Child Sexual Exploitation Online." The Guide, which was published in 2013 for the benefit of technology companies, offered the following advice: "Activate your user base to become a second set of eyes and ears for your service. Make it easy for users to flag and report exploitative content or behavior. This should include educating your users about forms of exploitation, the warning signs and making it easy across platforms to report photos, links, users, ads and other suspicious behavior."

Know Your Customer
Usually advice is given to the potential customer of file sharing services to perform due diligence before they commit to sending their data to a service provider. By the same token, it behooves the file sharing/hosting company to gather background on prospective customers. As noted by the PCI Security Standards Council of the financial industry, without such knowledge the file sharing company may not be aware of "issues within the client environment that could impact their service provision".

Data Retention Practices
Both for Internet Service Providers and file sharing companies, data retention and preservation are critical functions in the fight against child pornography. File sharing companies should strongly consider logging IP's and discouraging/preventing a customer's use of proxies to log onto a company's URL.

Repeat Offender Policy

In its "Responsible Practices" published in 2012, RapidShare offered guidelines for file hosting companies to address copyright infringement issues. Although the references are to "infringers," much of this guidance can be applied to keeping child sexual exploitation material off of a company's platform:

- *Service providers should make efforts to detect repeated efforts by users to store materials that the service provider previously deleted or disabled based on takedown notices, unless the users provided properly formed counter-notifications. This means that service providers must determine, to the extent technically feasible, unique signatures of disabled files and scan new files for identical signatures.*

RapidShare's "Responsible Practices" also suggest:

- *Expeditious removal or disabling of access to infringing material or activity when the provider gains knowledge of an infringement or facts or circumstances make the infringement apparent.*
- *Services should require valid e-mail addresses of subscribers and account holders in order for them to register new accounts. The service should periodically test the validity of subscriber e-mail addresses and require updating of obsolete email addresses in its system.*

High-Risk Practices

There are certain practices that put file hosting and sharing companies at risk of being abused by those who have illegitimate interests or criminal intentions. These practices, which should be avoided, include:

- "Rewards," cash payments, affiliate programs, advertising revenue or other incentives are paid based on the number of times files are downloaded, streamed or otherwise accessed.

- Links to prohibited content are indexed or distributed on third party websites or search engines.

- The site provides a "link checker" which allows uploaders to check if a link has been disabled to facilitate re-upload of content already removed.

- The site provides uploaders with "forum codes" and "URL codes" to facilitate incorporation of the links on third party indexing or "linking" websites.

POTENTIAL DETECTION PRACTICES

Leaders in the fight against child pornography employ a variety of methods to proactively detect the illicit content on their systems.

Some organizations use "keyword" lists in multiple languages and build them into detection tools or systems to proactively block, detect or flag for review potential child sexual exploitation content. For maximum effectiveness, keywords and modeling techniques should be updated at least weekly or, if a company has the resources and technology for real-time scanning, that option should be used.

Companies also employ tools that crawl and/or spider systems internally and externally on the web looking for policy violations. One tool to consider is PhotoDNA, an image-matching technology developed by Microsoft Research in collaboration with Dartmouth College. It creates a unique signature for a digital image, something like a fingerprint, which can be compared with the signatures of other images to find copies of that image. NCMEC and online service providers such as Microsoft and Facebook currently use PhotoDNA to block known PhotoDNA images upon upload and help detect, report and ultimately eliminate some of the worst known images of child pornography online, helping identify thousands of these images that would previously have gone undetected.

Another way to crawl internal systems is to review connections between known child abuse material accounts. The accounts of users who are connected to known abuse through downloads, shared access or uploads can be flagged for manual review.

Companies can also use INTERPOL's "Worst of" Child Abuse URL list to proactively block links and uploads. The list is maintained and updated weekly by INTERPOL and sent to all interested parties free of charge. Facebook uses the list to effectively blacklist all the URLs contained in the list from being uploaded, shared or otherwise linked from its network.

Other tools that companies use include file matching technologies and hash files with various algorithm schemes.

CONCLUSION

The fight against child pornography is always evolving as perpetrators are constantly seeking ways to leverage new technologies to avoid detection. Responsible companies in the file sharing and file hosting segments are interested in implementing procedures to avoid being abused by those who seek to sexually exploit children. It is the hope of the International Centre for Missing & Exploited Children and the APAC-FCACP that these guidelines will contribute to those efforts. The APAC-FCACP will continue in its mission to support the file hosting/sharing industry and others in the battle against child pornography.

For more information write to information@icmec.org.

ADDENDUM

The Reporting Process and Hotlines

As noted previously, companies should establish processes to manage receiving abuse reports of users of their service storing, hosting or sharing suspected child sexual exploitation content. A process should be implemented to investigate these types of reports and collect, preserve and report relevant information through the appropriate channel based on applicable laws or process for the location of the company.

For example, companies based in the United States are legally obligated to report apparent child pornography they find on their systems to the National Center for Missing & Exploited Children (www.cybertipline.com; 1-800-843-5678). NCMEC is a private, nonprofit organization that serves as the resource for the United States on the issues of missing and sexually exploited children.

NCMEC's sister agency, the International Centre for Missing & Exploited Children is a resource to help companies outside the U.S. identify and develop reporting protocols and processes. Write to information@icmec.org. ICMEC has done extensive research on child pornography laws outside the United States. ICMEC's report - *Child Pornography: Model Legislation & Global Review* - can be found at www.icmec.org.

Additionally, companies based outside the U.S. can research if a hotline exists in their country by visiting the website of the International Association of Internet Hotlines (INHOPE, www.inhope.org). INHOPE coordinates a network of Internet Hotlines all over the world, supporting them in responding to reports of illegal content to make the Internet safer.

INHOPE Hotlines offer the public a way of anonymously reporting Internet material including child sexual abuse material they suspect to be illegal. The Hotline will ensure that the matter is investigated and if found to be illegal the information will be passed to the relevant Law Enforcement Agency and in many cases the Internet Service Provider hosting the content.

Here is a sampling of reporting mechanisms in several countries. Visit the INHOPE website for more information www.inhope.org. If your country does not have a hotline, you can contact local law enforcement if you suspect that there is child pornography on your system.

Australia

The Australian Communications and Media Authority (ACMA)

Email: online@acma.gov.au, Website: www.acma.gov.au/hotline

The Australian Communications and Media Authority (ACMA) is a statutory authority within the Australian Government, responsible for the regulation of broadcasting, the internet, radio communications and telecommunications. The ACMA administers a hotline as legislated and

conducts investigations into online content as part of the Online Content Co-regulatory Scheme[1] in place under the *Broadcasting Services Act 1992*.

The ACMA Hotline investigates complaints about potential illegal online content and other prohibited content. The ACMA Hotline gives priority to complaints about online child sexual abuse material and other potentially illegal content.

Canada

The Canadian Centre for Child Protection

Telephone: +1 204-945-5735, Website: www.cybertip.ca

The Canadian Centre for Child Protection, a charitable organization dedicated to the personal safety of all children, operates Cybertip.ca, Canada's national tipline for reporting the online sexual exploitation of children. Cybertip.ca has been in operation since September 26, 2002 and was adopted under the Government of Canada's *National Strategy for the Protection of Children from Sexual Exploitation on the Internet* in May 2004.

Mandatory Reporting

Website: https://www.cybertip.ca/app/en/projects-mandatory_reporting

On December 8, 2011, Bill C-22, *An Act Respecting the Mandatory Reporting of Internet Child Pornography by Persons who Provide an Internet Service*, came into force. This federal legislation requires all persons who provide an Internet service to report any incident of Internet child pornography. Under section 2 of the regulations, the Canadian Centre for Child Protection (through the Cybertip.ca program) was named the designated reporting entity.

Germany

Two hotlines operate in Germany, and both are members of INHOPE.

The Verband der deutschen Internetwirtschaft - eco *(association of German internet enterprises)*

Website: http://www.internet-beschwerdestelle.de/en/aboutus/index.htm

Founded in 1993, eco is the foundation of the first commercial internet service providers (ISP) in Germany. In 1995, the "eco forum" was officially noted in the register of associations in Bonn (no VR 6973). Since then, the association has developed and has established itself as an acknowledged stakeholder, significantly contributing to the German Information and Communication Services Act (Information- und Kommunikationsdienste-Gesetz, IuKDG).

[1] The co-regulatory scheme is underpinned by the National Classification Scheme that applies to traditional media platforms in Australia such as cinema, DVDs, computer games and publications. The National Classification Scheme requires assessment of material based on the impact of the classifiable elements of sex, violence, nudity, themes, language and drug use. The National Classification Scheme gives effect to certain principles, including that adults should be able to read, hear and see what they want and minors should be protected from material likely to harm or disturb them.

Since 1997/98 with the foundation of the Internet Content Task Force (ICTF) and the foundation of the Voluntary Self-Monitoring of Multimedia Providers (FSM), eco participates actively in the development of the German system of self-regulation of that industry.

Voluntary Self-Monitoring of Multimedia Providers (FSM)

The Voluntary Self-Monitoring of Multimedia Providers (FSM e.V) is a non-profit association founded in 1997 by the associations of media and telecommunication companies which provide online services and companies that are online content, host or access providers. FSM is committed to youth protection on the internet and to combating illegal content in online media. Every internet user can make a complaint to the FSM, free of charge, about illegal internet content. The staff investigates every complaint for possible contravention of the codes of conduct of the FSM. This essentially covers provisions of penal law, youth protection and conformity with accepted journalistic principles. The hotline deals in particular with complaints against the following kinds of content:

Complaints Procedure

Complaint Mechanism: http://www.internet-beschwerdestelle.de/en/

The complaints procedure is governed by the following rules of FSM and the Association of German ISP and Internet Association. The two associations are responsible for the following areas:

FSM e. V.:

- web content
- content of mobile radio which is accessible via internet
- age verification systems (AVS)
- Chat

eco e.V.:

- Newsgroups
- Spam / E-Mail
- Bulletin Boards
- ICRA-Labels
- peer-to-peer (P2P)

Japan

Internet Association Japan

Email: japan@internethotline.jp, *Website:* www.internethotline.jp

The Internet Hotline Center (IHC), setup in June 2006 and housed within the Internet Association of Japan, accepts reports of illegal and harmful content against public safety and social order on the Internet from Internet users. It is a member of INHOPE since March 2007. IHC analyzes all reports received, and illegal and harmful information is forwarded to the National Police Agency, and then to ISPs for removal. In some cases, legal advice is sought for professional determination. The IHC does not deal with violations of intellectual property (copyrights and trademarks infringement), defamation and slander.

Netherlands

The "Meldpunt ter bestrijding van Kinderpornografie op Internet"

Email: info@meldpunt-kinderporno.nl, Website: http://www.meldpunt-kinderporno.nl/EN/about_us.htm

The "Meldpunt ter bestrijding van Kinderpornografie op Internet" [the Hotline combating Child Pornography on the Internet] is an independent private foundation, officially opened by the Ministry of Justice in June 1996. The main objective of the hotline is to contribute to the reduction of the distribution of child abuse images via the Internet.

Taiwan

ECPAT Taiwan

Email:web547@ecpat.org.tw, Website: http://www.web547.org.tw

ECPAT Taiwan launched an Internet reporting hotline, Web547, on July 21st 1999, to make the Internet a safer place, and to ensure children's online safety. Web547 is set up to receive reports on illegal and harmful information from Internet users. （the name Web547 means "no pornography on websites." The Chinese pronunciation of 547 sounds similar to the Chinese words for "no pornography".）

To remove and eliminate illegal and harmful information on the Internet, Web547 cooperates with the police, ISPs and other competent authorities. Child pornography (child sexual abuse content) is a serious online problem and Web547 transmits reports of this type of content directly to the 9th Investigation Brigade of the Central Investigation Bureau Division of the Taiwanese National Police for further investigation.

Furthermore, due to the anonymous and transnational nature of the Internet, international cooperation is also needed. Therefore, if the reported site is hosted in a foreign country, Web547 will forward the information to the INHOPE hotline network.

Switzerland

The Swiss Coordination Unit for Cybercrime Control (CYCO)

Website: http://www.cybercrime.admin.ch/content/kobik/en/home/meldeformular.html

Switzerland does not have an INHOPE member hotline, however the Swiss Coordination Unit for Cybercrime Control (CYCO), which was founded in 2001 and is part of the Federal Office of Police, is the central office where people can report suspect Internet crimes. After an initial examination of the report and safeguarding of data, the report is forwarded to the respective local or foreign law enforcement. CYCO also takes active part in the search for criminal subject matter on the Internet and is responsible for in-depth analysis of cybercrime. A form for complaints in English appears on its homepage.

ActionInnocence

Website: http://www.actioninnocence.org/suisse/web/home.aspx?page=83

Also in Switzerland, Action Innocence provides solutions to law enforcement agencies for the tracking of child pornography online, runs workshops to raise awareness with children and operates awareness-raising campaigns through the media. To find out more go to their website above (Source – FOSI: http://www.fosigrid.org/europe/switzerland)

United States

The National Center for Missing & Exploited Children (NCMEC)

Website: www.cybertipline.com, Telephone: 1-800-843-5678

The National Center for Missing & Exploited Children (NCMEC) is a private, nonprofit organization that serves as the resource for the United States on the issues of missing and sexually exploited children. Under its Congressional mandate, NCMEC operates the CyberTipline, the national clearinghouse for leads and tips regarding crimes against children on the Internet. It receives reports in eight categories of crimes against children.

These reports are made by both the public and by U.S.-based electronic communication service providers and remote computing service providers, who are required by law to report apparent child pornography to law enforcement via the CyberTipline (18 U.S.C. §2258A).

A company can report suspected child exploitation incidents to www.cybertipline.com or 1-800-843-5678 along with the company's mailing address, telephone number, facsimile number, and the electronic mail address of an individual point of contact at the company. NCMEC also has a bulk reporting mechanism, for companies that handle a high volume of reports.