THORN

SOUND PRACTICES GUIDE

To Fight Child Sexual Exploitation Online

thorn™

AUGUST 2014

TABLE OF CONTENTS

OVERVIEW

THE GOAL OF THE THORN SOUND PRACTICES GUIDE IS TO HELP TECHNOLOGY COMPANIES IDENTIFY TOOLS AND PRACTICES THAT CAN HELP PREVENT THEIR PLATFORMS FROM BEING USED FOR CHILD SEXUAL EXPLOITATION.

Specifically, this document outlines sound practices that are voluntarily being deployed across the industry in order to prevent, identify, report and remove child sexual abuse and sexual exploitation content. Companies can use this document as a resource to learn what others are doing, to identify new tools to implement and, as this will be an ever-changing document, to suggest new and improved tools for the industry to use. This document is not reflective of all contributing partners' practices. This guide should be seen as informational, not prescriptive – companies can implement some, but not necessarily all of the suggestions below.

IMPORTANT: **This document does not constitute legal advice, and readers should not rely on this information without seeking legal advice from a licensed attorney.**

METHODOLOGY

THORN DEVELOPED THE SOUND PRACTICES GUIDE WITH INPUT AND COLLABORATION FROM **MICROSOFT, TWITTER, GOOGLE, FACEBOOK, PINTEREST, WEPAY,**

and other technology companies with experience combating child sexual exploitation on their platforms, as well as NGOs who have worked in this space. The input of these contributing partners was critical to developing a comprehensive set of tools, resources and suggested policies.

CHILD SEXUAL EXPLOITATION AS DEFINED HERE INCLUDES **PRODUCTION, SOLICITATION, DISTRIBUTION, RECEIPT, AND POSSESSION OF CHILD PORNOGRAPHY** (ALSO CALLED CHILD SEXUAL ABUSE MATERIAL); ONLINE ENTICEMENT OF CHILDREN FOR SEXUAL ACTS; CHILD SEX TRAFFICKING; AND CHILD SEX TOURISM, ALL OF WHICH ARE ILLEGAL UNDER US LAW.

A minor is defined as a person under the age of 18 for the purposes of this report. Complete legal definitions and associated laws are referenced in the appendix. Note that tools outlined here are more focused on addressing child sexual abuse material rather than other forms of child sexual exploitation, due to the fact that more tools focused on identifying and removing child sexual abuse material exist. However, at the end of this document, we outline proposed concepts for helping to more thoroughly address the issues of online enticement, child sex trafficking and child sex tourism.

CHILD PORNOGRAPHY IS ILLEGAL UNDER FEDERAL LAW AND IS DEFINED AS the visual depiction of a minor engaging in sexually explicit conduct. (See 18 U.S.C. § 2256.) The definition includes images depicting lascivious exhibition of children's genitalia. Many court cases use "Dost factors" (named after the case of U.S. v. Dost from 1986, at 636 F. Supp. 82 (S.D. Cal. 1986)) to determine whether an image constitutes lascivious exhibition. Dost factors are outlined in the Appendix. It is illegal to produce, solicit, distribute, receive, or possess child pornography. (See 18 U.S.C. § 2251, 2252, 2252A.)

ONLINE ENTICEMENT OF CHILDREN FOR SEXUAL ACTS IS ILLEGAL UNDER FEDERAL LAW and includes inducing, enticing, or coercing a minor to engage in sexual activity. (See 18 U.S.C. § 2422.)

CHILD SEX TRAFFICKING IS ILLEGAL UNDER FEDERAL LAW and is defined as knowingly recruiting, enticing, harboring, transporting, providing, obtaining, or maintaining a minor, knowing that the minor would be caused to engage in a commercial sex act. (See 18 U.S.C. § 1591.)

CHILD SEX TOURISM IS ILLEGAL UNDER FEDERAL LAW and is defined as traveling to another state or country to engage in illicit sexual conduct (including sex acts with minors). (See 18 U.S.C. § 2423.)

LEGAL CONSIDERATIONS

The following is a general description of the law related to when a company can be considered to be an agent of law enforcement. As noted above, this isn't legal advice and readers should not rely on this information without seeking legal advice from a licensed attorney.

In the United States, a person has the right to be protected by the Fourth Amendment from unreasonable search and seizure by the government. A search of a private account requires a search warrant supported by probable cause. If the government undertakes a search without such a warrant, the information discovered or derived from that search cannot be admissible in court.

While the Fourth Amendment is intended to only apply to the government, it can be extended to private entities when they appear to take on the role of the government. Hence, if a company takes certain actions primarily to fulfill a law enforcement purpose, it may be deemed to be an agent of the government, and subject to the same liability as a government actor for searching an account without first obtaining a search warrant.

One of the key factors a court will look to is whether the company had a private, non-government purpose in searching the user's account, and whether the company's actions were instigated or controlled by law enforcement. This distinction between private and government purpose is important to keep in mind within a company's security operations.

It may be useful to create a company policy that recognizes these agency issues, and reinforces the company's legitimate purposes in securing its platform. Some helpful policy suggestions include:

1. Draft a formal company policy document that sets forth what the private purpose behind the child safety program is.

2. Ensure that any and all disclosure of user data to law enforcement is done pursuant to law.

3. To the extent a company undertakes an investigation of an account, try to make sure that it is done without the government's concurrent instigation, control, or knowledge, and documented accordingly.

4. Seek legal counsel to ensure decision-makers are well versed on the latest developments in this field.

UNIVERSAL TOOLS

The following is a list of resources, tools, and processes that can be applied across multiple types of services and that provides a good foundation for most companies who are working to fight exploitation on their platforms. In the next section, we will discuss sound practices by service and highlight practices that may be unique to a given type of platform or service. It is important to note that while combating the exploitation of children is important, so is user privacy and security. Tools that are built and used should respect privacy policies.

INDUSTRY DEFINITION: Many technology companies have worked hard over the past few years to create industry standard definitions of categories of child sexual abuse material, so that they can share information with one another using a common language. Industry classification, which was based on Dost factors, the Tanner Scale, company-specific experience around what to look for, and risk factors, has enabled tech companies to work together to ensure that the problem can be addressed as seamlessly as possible.

TERMS OF SERVICE: Ensure that language is included in Terms of Service that prohibits your service from being used for the exploitation of minors. Stronger language can include prohibiting pornography and more specifically, child sexual exploitation on your platform. This will notify users at the outset that your platform does not allow this type of content and that when it is identified, it will be removed and reported.

USER FLAGGING: 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.

NATIONAL CENTER FOR MISSING AND EXPLOITED CHILDREN (NCMEC) CYBERTIPLINE: Since 1998, NCMEC has operated the CyberTipline, a reporting mechanism for suspected child sexual exploitation. The CyberTipline accepts reports on the following: Child Pornography, Online Enticement of Children for Sexual Acts, Child Sex Trafficking, Child Sex Tourism, Unsolicited Obscene Material Sent to a Child, Misleading Domain Names, and Misleading Words or Digital Images on the Internet. The CyberTipline was authorized by Congress to receive reports of apparent child pornography from electronic communication service providers and remote computing service providers. (See 18 U.S.C. § 2258A.) To that end, NCMEC created a secure reporting form specifically for use by electronic service providers (ESPs). The reporting form allows ESPs to upload images or videos of apparent child pornography. In addition, ESPs can provide suspect and incident information, which CyberTipline analysts use to attempt to locate a jurisdiction where the report can be made available to law enforcement for possible investigation.
Contact: *espteam@ncmec.org*.

NCMEC'S NOTICE TRACKING SYSTEM: NCMEC has developed a notice tracking system, allowing them to notify ESPs when the CyberTipline receives reports with URLs containing the sexual exploitation of a minor that the ESP is hosting. Domestic companies usually remove this content within a few days. If the URL is hosted abroad, NCMEC notifies the INHOPE hotline.
Contact: *espteam@ncmec.org*.

NCMEC'S URL LIST: NCMEC manages a constantly-evolving URL list of web pages containing apparent child pornography content, namely, an image, whether a photograph or video, of a child victim engaged in sexually explicit conduct.

NCMEC currently provides a daily list of active web pages containing apparent child pornography to U.S.-based electronic service providers (ESPs) that have entered into a memorandum of understanding with NCMEC.

When a web page is reported to the CyberTipline, a NCMEC analyst visits the web page, verifies that it contains apparent child pornography and documents the content in the CyberTipline report. The completed report is made available to law enforcement for possible investigation. Each business day, NCMEC verifies that the web pages on the URL list contain apparent child pornography. A new list is generated each day and made available to participating ESPs. As the URL list is dynamic and changes each day, ESPs are encouraged to access the list daily.
Contact: *espteam@ncmec.org*.

PHOTODNA: In 2009, working with Dartmouth's Dr. Hany Farid, Microsoft developed PhotoDNA, a technology to aid in finding some of the"worst of the worst" images of child sexual exploitation on the Internet. Following Microsoft's donation of the PhotoDNA technology to NCMEC, NCMEC established a signature-based program for online service providers to help disrupt the spread of child sexual abuse material online. Implementing PhotoDNA can improve your company's ability to find child sexual abuse material, report it and remove it from your systems. This also reduces the cost of screening and the human impact on your staff of viewing this content. PhotoDNA creates a hash value of the visual characteristics of an image. That hash value can then be used to compare the image against a collection of images to find those that are visually similar. A company can compare photos against a set of hash values of known child sexual abuse material images, in order to identify child sexual abuse material and either prevent its upload or assist in prompt removal. This tool is much more advanced than MD5 or SHA1 hashes, which do not work if the user alters even one pixel of the image. PhotoDNA identifies many separate points within the image to ensure that even if an individual resizes, compresses, or otherwise modifies the image, it may still be identified as known child sexual abuse material.
To learn more, visit: *www.microsoftphotodna.com*.

For eligible electronic service providers, the PhotoDNA technology can be sublicensed for free from NCMEC. Once a company implements PhotoDNA technology, NCMEC can then provide that company with a set of PhotoDNA signatures of known child sexual abuse material images, which include an identified child or fall into the 'worst of the worst' category in which the child in the photo has not been identified.
Contact: *photodna@ncmec.org*.

REVIEW & REPORT PROCEDURES: Thorn encourages companies to be proactive in reducing child sexual exploitation on their systems. Build a relationship with NCMEC to understand the actions you should take upon finding content.

CHILD SEXUAL ABUSE MATERIAL KEYWORD LIST: Thorn manages a "child sexual abuse material keyword list" to help companies identify posts, websites, photos, videos, or other content that may contain child sexual abuse material and may warrant a safety review.
Contact: **Leah Treitman,** Thorn, *Programs@wearethorn.org*.

DETERRENCE PSAs FOR SEARCH ENGINES – CHILD SEXUAL ABUSE MATERIAL: Thorn has created PSAs that can be served against known search terms for child sexual abuse material. These PSAs are directed at those who may be searching for this illegal content and offers these people help with their compulsion. The PSA links to a page explaining the consequences of their actions and links to a help line associated with an organization that provides services for those with sexual compulsions.
Contact: **Leah Treitman,** Thorn, *Programs@wearethorn.org*.

EDUCATIONAL ONLINE PSAs – CHILD SEX TRAFFICKING: Thorn has created PSAs that can be used online to educate potential sex buyers about the signs and the consequences of sex trafficking, and reach potential victims with resources. These PSAs offer victims and others a hotline to call to either report an instance of trafficking or to seek help.
Contact: **Leah Treitman,** Thorn, *Programs@wearethorn.org*.

INDUSTRY HASH SHARING PLATFORM: Companies using PhotoDNA can share hash values of photos they have found with other companies, in order to more rapidly build a shared database of image hashes and, consequently, more rapidly remove this content from their systems. The result of this, beyond more rapid identification and removal, is the reduced human impact on front-line safety teams who have to view content, reduction in costs for teams scanning for images and more effective and efficient reporting to NCMEC, leading to more rapid victim identification. Contact NCMEC to participate in the Industry Hash Sharing Platform. If you are concerned your company does not have the bandwidth to participate in this system or would like assistance with implementation, Thorn can help.
Contact: **Leah Treitman,** Thorn, *Programs@wearethorn.org*. or
The ESP Team, NCMEC, *espteam@ncmec.org.*

IMPROVED RESOURCES FOR EMPLOYEE HEALTH: Constant exposure to child sexual exploitation images, video, and other content can be stressful for employees on the front lines. The technology coalition, in partnership with the International Center For Missing and Exploited Children, has written an "Employee Resilience Guide" that can be used to help address this problem.
To download it, visit: *http://bit.ly/UN1DmF*

PRACTICES BY SERVICE

This section outlines considerations for preventing, identifying, removing and reporting this content by type of service. These considerations were developed by reviewing existing procedures across multiple technology companies and by speaking with survivor organizations and NGOs. We believe that there is more that can be done and welcome suggestions for improvements and ideas for new tools. These steps should be utilized only in a manner that is appropriate for your service. This document does not constitute legal advice, and readers should not rely on this information without seeking legal advice from a licensed attorney.

PHOTO SHARING

The ultimate goal is to prevent photo and video sharing sites from hosting child sexual abuse material and other exploitative content, but this content still manages to find its way onto these services. The below steps may help companies improve their ability to identify and rapidly remove child sexual abuse material, as well as prevent their systems from being used for exploitation.

1. **TERMS OF SERVICE:** Clearly articulate in your terms of service that your platform does not allow child sexual abuse (child pornography)/child abuse material content) and that when it is identified, it will be removed and reported.

2. **PRE-SCREEN PHOTOS:** Use PhotoDNA or another photo hash system to pre-screen photos against a known set of illegal child sexual abuse images at upload to help prevent the content from appearing on your system.

3. **SCREEN PHOTOS AT REST:** Use PhotoDNA or another photo hash system to proactively screen photos at rest against a known set of illegal child sexual abuse images. If known child sexual abuse material photos are found, you may be able to do manual forensics on the account and associated accounts to see if more illegal images are found and to ensure a full report to NCMEC and law enforcement.

4. **SCREEN VIDEOS:** See "Opportunities" section for new developments on automated video detection and hash sharing.

5. **ACTIVATE YOUR USER BASE:** Give your users an easy and visible tool to report inappropriate photo and video content.

6. **IDENTIFY HIGH-RISK USERS:** If your service is able to do so, leverage sex offender registry information to identify high-risk users. In doing so, make sure you always have a current list as it can change frequently.

7. **REPORT:** Build a relationship with NCMEC to establish an appropriate process for rapid reporting.

8. **PREPARE FOR THE LAW ENFORCEMENT RESPONSE:** Develop an internal process to expedite the response to law enforcement subpoenas, court orders, etc. Having a 24/7 contact mechanism for law enforcement to use only during emergent situations may also be helpful. It may also be useful to create a law enforcement compliance guide. Many companies already have guides available online, so it may be valuable to consult and collaborate with colleagues and peers, including NCMEC, before developing your own.

CASE STUDY: Company A, an international site with a large photo sharing service, originally had a manual review and report process for identifying child exploitation material. This process was slow and necessarily exposed staff to this illicit content. PhotoDNA has made this process significantly more efficient and thorough, increasing the amount of material

Company A can refer to the National Center for Missing and Exploited Children, while decreasing the number of images staff must review. In the first month of PhotoDNA's operation, Company A was able to send ten times as many illegal images to NCMEC as in previous months; more importantly, PhotoDNA allowed the company to make these reports automatically at upload time, expediting the report to law enforcement and reducing the amount of time employees spend on manual reporting. Thanks to these efficiency gains, Company A has been able to put more time toward fighting new child exploitation material on their service, knowing that their staff will not be continuously exposed to known images.

SOCIAL NETWORKS

Some of the sound practices for social networks are included in the "Photo Sharing" section, but there's also the potential for link sharing within social networks. Additionally, social networks may be used to advertise or recruit victims of human trafficking.

1. CHILD PORNOGRAPHY/CHILD SEXUAL ABUSE MATERIAL

   A. **TERMS OF SERVICE:** Clearly articulate in your terms of service that your platform does not allow child sexual abuse (child pornography)/child sexual exploitation content and that when it is identified, it will be removed and reported. Pay close attention to the language that you use, as users may understand terms differently.

   B. **PRE-SCREEN PHOTOS:** Use PhotoDNA or another photo hash system to pre-screen photos against a known set of illegal child sexual abuse images at upload to help prevent the content from appearing on your system.

   C. **SCREEN PHOTOS AT REST:** Use PhotoDNA or another photo hash system to proactively screen photos at rest against a known set of illegal child sexual abuse images. If known child sexual abuse images are found, you may be able to do manual forensics on the account and associated accounts to see if more illegal images are found and to ensure a full report to NCMEC.

   D. **ACTIVATE YOUR USER BASE:** Give your users an easy and visible tool to report inappropriate content. Increasing the granularity of descriptions available within your reporting options may help you more rapidly assess and manage the situation. Allowing users to describe why they are reporting the content and providing pre-categorized options may help ensure that reports are sent to the appropriate team within your company.

   E. **IDENTIFY HIGH-RISK USERS:** If your service is able to do so, leverage sex offender registry information to identify high-risk users. In doing so, make sure you always have a current list as it can change frequently.

   F. **PROACTIVELY REMOVE LINKS:** Leverage the NCMEC URL list on a daily basis to remove links that host known child sexual abuse material.

   G. **REPORT:** Build a relationship with NCMEC to establish an appropriate process for rapid reporting.

2. CHILD SEX TRAFFICKING

   There is evidence that suggests that social networks are used to "groom" potential victims of sex trafficking. The methods are varied, but in many cases a trafficker may befriend the victim via the social network and send

the individual messages in order to develop a relationship that can result in a trafficking situation. Additionally, platforms within social networks can be used to advertise victims of sex trafficking. Anecdotally, these are referred to as "pimp" pages, and they are set up so that pimps can advertise the victim to a targeted group of sex buyers at once and communicate with them on one platform. Traffickers have also been known to use the geo-location services available within social networking sites by requiring their victims to "check in" at specific times, which enables the pimp to know their exact location.

While there is a need for better tools to combat this type of exploitation on social networks, there are a few current recommendations:

A. **SCREEN FOR KNOWN TRAFFICKING TERMS AND BEHAVIORS:** Employ automated scanning for key terms or phrases known to be associated with sex trafficking and subsequent manual review of those users or pages. Traffickers may use known prostitution slang terms in posts and photo captions. They also may have images of their victims photographed with branding or tattoos. All of this information could be useful after a profile is found through automated scans for key terms or phrases.

B. **SCAN FOR OUTLIER FRIEND PATTERNS:** If the user's age can be determined, create algorithms to flag users over a certain age who befriend numerous underage individuals, or send messages to many strangers. Even if the user's age is not known, individuals whose friend requests are rejected at a high rate can be flagged for review.

C. **MONITOR FOR FALSE PROFILES:** Monitor age and name changes to ensure that users are not falsely representing themselves.

D. **ENSURE THAT THE PRIVACY OF MINORS IS PROTECTED:** If your service has age data about its users, educate minors about how to protect their privacy and consider putting additional safeguards in place for minors. One way of doing so is to ensure that photos of minors do not appear in public search results and that they are not accidentally sharing their location, photos, or other personally identifying information with people outside their networks.

E. **PROACTIVELY COMMUNICATE WITH USERS:** Inform users about how to keep themselves safe from situations that may lead to sexual exploitation. See Appendix B for an example from Facebook that illustrates how you can communicate with users about what to do in these situations.

F. **REPORT:** Build a relationship with NCMEC to establish an appropriate process for rapid reporting. Although the legal obligation to report is related to child pornography, the CyberTipline also receives reports related to possible child sex trafficking situations.

SEARCH ENGINES

Search engines are not liable for search results that present illegal content; however, it is in the best interest of any company to keep users from using their site for illegal purposes. In relation to child sexual exploitation, search engines can be used to surface child sexual abuse material, facilitate child sex trafficking and engage in child sex tourism. The below practices illustrate how search engines can mitigate the problem of serving results that contain illegal content as well as deter users from searching for illegal content on a given network.

1. **PROACTIVELY REMOVE LINKS:** Leverage the NCMEC URL list on a daily basis to remove links that host known child sexual abuse material.

2. **PROACTIVELY SCREEN PHOTOS:** Use PhotoDNA or another photo hash system to proactively screen photos that are served in search results against a known set of illegal child sexual abuse images and remove/report them.

3. **ACTIVATE USER BASE:** Create an easy and visible way for users to report links or content that is served via your search engine.

4. **DETERRENCE ADS:** When a user searches for child sexual abuse material or other exploitative content, it is possible to serve a PSA that will offer that user help.

5. **REVIEW & REPORT:** If an electronic service provider finds a link, photo or other content containing the sexual exploitation of a minor, it can be reported to law enforcement via the National Center for Missing and Exploited Children's CyberTipline (*www.cybertipline.com*)

6. **COLLABORATE:** Take proactive efforts to inform other search engines of the links and images that you find and remove from your search index. This may limit the amount of duplicate work performed.

CASE STUDY: Thorn has developed deterrence ads aimed at those searching for child sexual abuse material, which have been served millions of times across four search engines over a period of three years. Additionally, the ads have seen a 3% click-through rate from people seeking help after searching for exploitative material.

CLOUD FILE STORAGE

As more individuals and companies begin to use cloud file storage, it presents another environment for people to store child sexual abuse material, as well as an opportunity for service providers to find this content, remove it and report to NCMEC.

1. **TERMS OF SERVICE:** Clearly articulate in your terms of service that your platform does not allow child sexual abuse (child pornography)/child sexual exploitation content and that when it is identified, it will be removed and reported.

2. **PRE-SCREEN PHOTOS**: Use PhotoDNA or another photo hash system to pre-screen photos against a known set of illegal child sexual abuse images at upload to help prevent the content from ever being stored in your system.

3. **SCREEN PHOTOS AT REST:** Use PhotoDNA or another photo hash system to proactively screen photos at rest against a known set of illegal child sexual abuse images. If known child sexual abuse images are found, you may be able to do manual forensics on the account and associated accounts to see if more illegal images are found and to ensure a full report to NCMEC and law enforcement.

4. **ACTIVATE YOUR USER BASE:** Give your users and those who receive shared material from your users an easy and visible tool to report inappropriate content.

5. **IDENTIFY HIGH-RISK USERS:** If your service is able to do so, leverage sex offender registry information to identify high-risk users. In doing so, make sure you always have a current list as it can change frequently.

6. **REPORT:** Build a relationship with NCMEC to establish an appropriate process for rapid reporting.

CASE STUDY: As a participant in NCMEC's PhotoDNA Initiative, Microsoft implemented the PhotoDNA technology on its services, including Bing and OneDrive, its cloud solution, to compare images publicly shared or found on these services with the hash list from NCMEC. This implementation was a thoughtful and gradual process in order to validate the testing of the technology and to verify that the right processes were in place as matches were identified.

The implementation of PhotoDNA started with the indexing process for image search in Bing (in order to help prevent Bing from rendering these child sexual abuse images in its image search results) and on newly uploaded photos on OneDrive (to better disrupt the abuse of OneDrive for sharing these images). These deployments are worldwide. Thus far, Microsoft has found:

- Beginning in late 2010, OneDrive steadily increased the number of NCMEC signatures it was using, from 500 signatures in January 2011 to the full set of over 20,000 signatures offered by NCMEC.

- Beginning in March 2010, they implemented PhotoDNA onto Bing using 3,000 signatures from NCMEC. They are now using the full set of over 20,000 signatures offered by NCMEC. When they find a match in Bing, they report the URL to NCMEC.

- In addition to scanning images indexed by Bing, any additional images that Bing examines as they surface images from the internet are also compared to the full set of hashes currently offered by NCMEC.

- Today, Microsoft uses PhotoDNA to scan billions of images every day, identifying tens of thousands of matches to NCMEC signatures each year. These numbers are expected to increase as PhotoDNA continues to be deployed onto these services and as the size of the signature set expands with the introduction of the Industry Hash Sharing Platform described in the Universal Tools section.

CLASSIFIED SITES/ESCORT SITES

Classified sites and escort services sites have become an online destination for traffickers to sell victims, including those who are underage. Classified sites don't have a legal obligation to identify and prevent this behavior. However, if a classified site wants to ensure that their platform is not used for exploitation, there are a number of steps that can be taken.

1. **TERMS OF SERVICE:** Clearly articulate in your terms of service that your platform does not allow child sexual abuse (child pornography)/child sexual abuse material) and that when it is identified, it will be removed and reported.

2. **REQUIRE IDENTIFICATION:** Classified sites can require each poster to pay via credit card, so that each post is linked back to a financial transaction. If it is possible, you can prevent the use of prepaid credit cards, as this allows users to remain anonymous. Another option is to require posters to come into their corporate office, or to scan and send in a photocopy of their state-issued photo ID. Police say this can be helpful when investigating suspicious posts or posts involving known child victims, because each posting is linked back to a true identity. Requiring an "account" also makes it easier for the company to trace suspicious activity to a single account over time.

3. **PRE-SCREEN CONTENT:** Another option is for classified sites to ensure that each post is pre-screened before it is ever posted online. If using manual screeners, equip them with indicators of an underage victim of trafficking. While screening look for suspicious patterns, such as a single user/email address/credit card being used to post multiple ads depicting different individuals, which could escalate those ads for review. Another option is to have some manual screening in place and review these results through automation using patterns and indicators that can be learned by a machine.

4. **EDUCATION:** Educate all users of the site – posters and purchasers – about the issue of trafficking and give them the resources necessary to be vigilant in reporting suspected instances of trafficking. Run PSAs throughout the site educating users about the signs of trafficking and asking them to report suspicious ads. Also, provide resources for potential victims on the site – running ads with the national anti-trafficking hotline number to remind victims who may be forced to post themselves that there is help. Thorn has created these graphic ads and will share them free of charge with any classified site that requests them.
   To obtain these ads, please contact *Programs@wearethorn.org*.

5. **USER FLAGGING:** Provide an easy 'click to report' function for those browsing the site to report suspicious ads.

6. **REPORT:** Report any suspicious ads to law enforcement via the National Center for Missing and Exploited Children's CyberTipline and remove the ad, while retaining the information for law enforcement.

CASE STUDY: Geebo, a classified site committed to keeping sexual exploitation off its platform, has never had a case involving child sexual exploitation. They manage to do this in part because of their pre-screening process. Other sites without stringent measures in place have seen their sites used for the forced sale of minors for sex. (*Source:* National Center for Missing and Exploited Children)

EMAIL

E-mail can be used to share child sexual abuse images and links, but due to concerns over wiretap laws some companies are not finding, removing or reporting child sexual abuse material shared through email. This type of screening and prevention must be done carefully - the company must explicitly state their activities in its Terms of Service. Companies are able to disable URLs related to malicious software, so the potential to do the same for URLs on NCMEC's list exists – it's a matter of companies choosing to implement this policy and doing so with the proper processes.

1. **TERMS OF SERVICE:** Clearly articulate in your terms of service that your service prohibits the exploitation of minors in any form. Explain that sharing child pornography files is a violation of the terms of service and define child pornography using federal definitions.

2. **PRE-SCREEN PHOTOS:** Use PhotoDNA or another photo hash system to pre-screen photos against a known set of illegal child sexual abuse images upon upload before they are transmitted in order to help prevent the content from being sent through the system in the first place. If known child sexual abuse images are found, you may be able to do manual forensics on the account and associated accounts to see if more illegal images are found and to ensure a full report to NCMEC.

3. **PROACTIVELY REMOVE LINKS:** Leverage the NCMEC URL list on a daily basis to flag or disable links that host known child sexual abuse material.

4. **ACTIVATE YOUR USER BASE:** Give your users and those who receive shared material from your users an easy and visible tool to report inappropriate content. It may be helpful to add more granularity within your reporting options, so that the specific issue is brought to the attention of the correct team more rapidly.

5. **IDENTIFY HIGH-RISK USERS:** If your service is able to do so, leverage sex offender registry information to identify high-risk users. In doing so, make sure you always have a current list as it can change frequently.

6. **REPORT:** Build a relationship with NCMEC to establish an appropriate process for rapid reporting.

MESSAGING AND CHAT

Messaging and chat applications can be used to share child sexual abuse images, videos, links, as well as other forms of child sexual exploitation, such as live streaming child abuse. Some are designed to communicate with existing friends, while others are designed around meeting new people, and in some cases, meeting offline. Some applications have also integrated ephemeral image and video technology, which has implications for evidence when it comes to child sexual exploitation content. Below are some steps that companies can take to ensure their platforms are as safe as possible.

1. **TERMS OF SERVICE:** Clearly articulate in your terms of service that your service prohibits the exploitation of minors in any form. Explain that sharing child pornography files is a violation of the terms of service and define child pornography using federal definitions.

2. **PRE-SCREEN PHOTOS:** Use PhotoDNA or another photo hash system to pre-screen photos against a known set of illegal child sexual abuse images upon upload before they are transmitted in order to help prevent the content from being sent through the system in the first place. If known child sexual abuse images are found, you may be able to do manual forensics on the account and associated accounts to see if more illegal images are found and to ensure a full report to NCMEC.

3. **PROACTIVELY REMOVE LINKS:** Leverage the NCMEC URL list on a daily basis to flag or disable links that host known child sexual abuse material.

4. **ACTIVATE YOUR USER BASE:** Give your users and those who receive shared material from your users an easy and visible tool to report inappropriate content. It may be helpful to add more granularity within your reporting options, so that the specific issue is brought to the attention of the correct team more rapidly.

5. **PROACTIVELY COMMUNICATE WITH USERS:** Inform users about how to keep themselves safe from situations that may lead to sexual exploitation. See the appendix for an example from Facebook that illustrates how you can communicate with users about what to do in these situations.

6. **IDENTIFY HIGH-RISK USERS:** If your service is able to do so, leverage sex offender registry information to identify high-risk users. In doing so, make sure you always have a current list as it can change frequently.

7. **REPORT:** Build a relationship with NCMEC to establish an appropriate process for rapid reporting.

GAMING

The gaming industry represents another outlet for individuals to store and share child pornography/child sexual abuse images. With a growing market, and the increasing Internet access and data storage capabilities, it is important for companies to protect their systems.

1. **PRE-SCREEN PHOTOS:** Use PhotoDNA or another photo hash system to pre-screen photos against a known set of illegal child sexual abuse images at upload to help prevent the content from appearing in your game or platform. Newly identified photos of child sexual abuse can be reported to NCMEC and may be included on the industry shared hash list.

2. **ACTIVATE YOUR USER BASE:** Give players an easy and visible in-game method for reporting user-generated content.

3. **USER-GENERATED CONTENT:** Disallow hyperlinks, and implement keyword filtering and/or blacklisting for chat and messaging features.

4. **SCANNING:** Automate scanning by leveraging known child sexual abuse material keywords and phrases, bad IPs, and NCMEC's URL list. This will help to identify users for subsequent manual review.

5. PRIVACY
   a. **Geo-location:** Ensure that any geo-location features which share location of players with one another are opt-in only.

   b. **Data collection:** If you are collecting player data from social networks or during game installation, do not surface, or allow players to search for other users in-game by real name or location.

   c. **Educate:** Inform parents and children about protecting their privacy and provide easy access to privacy controls in-game to prevent accidentally sharing their location, photos, or other personally identifying information with people outside their networks.

   d. **Report:** Build a relationship with NCMEC to establish an appropriate process for rapid reporting.

   e. **Collaborate:** If identified users are linked to social network sites or other platforms, share relevant data with those social networks and platforms.

PAYMENT SERVICES

Online payment service providers may want to take steps to ensure that their services are not used for people to profit from selling child sexual abuse images and videos.

1. **TERMS OF SERVICE:** Clearly articulate in your terms of service that your platform does not process payments for child sexual abuse material/child sexual exploitation content. Some companies have taken further precautions by not processing payment for any adult content at all.

2. **KNOW YOUR CUSTOMER:** Knowing your customer is important. Useful information may include their contact information, social security number, and birthdate. This information is usually collected from merchants, but it is useful to collect from customers as well.

3. **SCREEN CONTENT:** It may be useful to scan and review the merchant's website and all related links from the website. Additionally, use automated reviews to look for keywords, or manually review your payments.

4. **RISK ANALYSIS:** Consider factors including how much content the pages contain, the gender of the buyers, the price range of the product, if the payers are connected to the recipient on other platforms, and the location of the buyers.

5. **TRANSACTIONS:** Consider limiting the use of prepaid credit cards. This allows consumers to remain anonymous making further investigation into their identity more difficult.

6. **KNOW YOUR MERCHANT**: While many Merchant Applications gather significant relevant background information on the merchant such as its business model, products or services it offers, operations, locations, principals and other key personnel, it may be helpful to include additional information on the merchant business background and operations in your application. For additional suggestions, see the Internet Merchant Acquisition Best Practices in "Other Resources."

7. **VERIFICATION:** Verifying merchant-provided information may prove useful in assessing potential risk. For suggestions of specific information to verify, see the Internet Merchant Acquisition Best Practices in "Other Resources."

8. **RED FLAGS:** Being aware of potentially suspicious activity may be useful for protecting your platform. If the trading address is a private residence, the merchant website acts as an "Internet mall" hosting products and services provided by a variety of sources, principals appear to lack a clear understanding of the business, the address indicated on the credit report is a mail drop, the merchant uses a generic mail carrier for its e-mail address, the business was established for fewer than 90 days, or the merchant website is

not “live” at the time of application, it may be necessary to conduct further investigation.

9. **MONITOR:** Monitor merchants on an ongoing basis. Base the frequency of review on the risk assessment of your merchant and take note of variations in activity. Keep a comprehensive list of “adult merchants” that process on your system (if permitted by your own policies) and routinely monitor these accounts. Cross-reference any known adult merchants with card information to provide “linkage” to potentially illegal merchants.

10. **WORD SEARCHES:** Perform word searches at the merchant’s website, using Thorn’s keyword list or another keyword list that your organization has, related to activities that violate your terms of service.

CASE STUDY: In 2006, the National Center for Missing & Exploited Children (NCMEC) and its sister agency, the International Centre for Missing & Exploited Children (ICMEC) launched the Financial Coalition Against Child Pornography (FCACP). This group is made up of leading banks, credit card companies, and payment companies, including American Express, Citigroup, Paypal, and Bank of America – their members comprise nearly 90% of the U.S. payments industry. The mission of this group was to stop the commercial sale of child pornography online.

When the Financial Coalition was launched, it was common to see commercial child pornography website subscription prices of $29.95 per month, payable by credit card. As law enforcement investigations of commercial child pornography websites increased, the websites evolved, requiring alternative payment methods in a multi-layered verification process involving passwords and text messages. Additionally, the Financial Coalition has reported that some of these websites are refusing to accept credit cards from the United States.

Since the start of the FCACP, there has been a 50% drop in the number of unique commercial child pornography websites reported into the U.S. CyberTipline.

According to NCMEC, mainstream payment services have put safeguards in place that successfully prevented their platforms from being used to purchase child sexual exploitation content. While the U.S. Department of Treasury noted a remarkable decrease in the estimation of the scope of this global industry, child pornography is still a massive problem. (*Source:* National Center for Missing and Exploited Children)

Companies interested in joining the FCACP should contact: *information@icmec.org*

COMMUNICATION WITH USERS

There is no standard practice for communicating with users about these activities. How to handle each case from a user communication perspective is left to each company's discretion. Below are some options for how to handle users sharing known child sexual abuse material or engaging in other forms of child sexual exploitation, including the online enticement of minors.

1. **PREVENT IT:** When this is possible, some companies prevent certain content from being uploaded in the first place, but do not necessarily give users an explanation.

2. **REMOVE IT:** In other cases, companies remove the content and do nothing else in terms of messaging.

3. **WARN THE USER:** Some companies warn the user once they encounter this content. Warning messaging can vary – be sure to consult with legal counsel about the messaging that best suits your needs. It may be helpful to communicate with the user about why the content was removed, to inform the user that their action has been noted, which may prevent them from repeating the action.

4. **SUSPEND, BAN, OR BLOCK THE USER:** In other cases, the company may decide to suspend the user and investigate their account. In more extreme cases, banning the user from the site, the company may add his or her email address to a "blacklist." However, email addresses are plentiful, and sites are now working to find more permanent ways of removing a user from a site. In some cases, the company could ban a specific device, or could use NAT addresses or other identifiers to find a reoffending user. This is an area that needs to be explored in more depth.

OPPORTUNITIES

This section outlines some of the new tools, policies, and procedures that are currently being developed or explored, based on needs that have been identified in the field. This list of projects is constantly evolving and growing. To suggest ideas for new tools, or for more information about these projects, please contact Thorn.

1. SHARED VIDEO HASH SYSTEM

Now that the National Center for Missing and Exploited Children has adopted the Industry Hash Sharing Platform for photos, there is an opportunity to explore how this model can be applied to video identification. Multiple companies currently provide video hashing and identification services, and each uses a different type of fingerprinting technology for videos. Industry-wide collaboration on photos has shown early success, and continuing this cooperation on the video side, though perhaps more technically challenging, will have significant impact in helping companies surface known child sexual exploitation content and ensuring that companies are benefiting from one another's efforts in this realm, helping to surface videos more quickly for review and reporting them to NCMEC for victim identification. Thorn is working on bringing industry together to agree upon a common or shared solution. If you can help in any way, or want to be involved in this initiative, please reach out.
Contact: **Leah Treitman,** *Programs@wearethorn.org*.

2. IMPROVED RESOURCES FOR PREVENTION

There are currently a few organizations providing help and counseling to people who are tempted to engage in child sexual exploitation, but they are resource-constrained and in need of assistance in reaching these individuals. Improving preventive treatment options for potential offenders is critical to keeping children safe. One organization that provides this type of specialized assistance is Stop It Now.
To donate, visit *www.stopitnow.org/donate*.

APPENDIX A: RELEVANT LAWS

The following is a selection of laws to help define some of the topics discussed within this paper. It is not comprehensive and legal matters concerning these topics should be discussed with counsel.

TITLE 18 > PART I > CHAPTER 110 > § 2258A

§ 2258. REPORTING REQUIREMENTS OF ELECTRONIC COMMUNICATION SERVICE PROVIDERS AND REMOTE COMPUTING SERVICE PROVIDERS

(a) **DUTY TO REPORT.—**

(1) **In general.—** Whoever, while engaged in providing an electronic communication service or a remote computing service to the public through a facility or means of interstate or foreign commerce, obtains actual knowledge of any facts or circumstances described in paragraph

(2) shall, as soon as reasonably possible—

(A) provide to the CyberTipline of the National Center for Missing and Exploited Children, or any successor to the CyberTipline operated by such center, the mailing address, telephone number, facsimile number, electronic mail address of, and individual point of contact for, such electronic communication service provider or remote computing service provider; and

(B) make a report of such facts or circumstances to the CyberTipline, or any successor to the CyberTipline operated by such center.

(2) **Facts or circumstances.—** The facts or circumstances described in this paragraph are any facts or circumstances from which there is an apparent violation of—

(A) section 2251, 2251A, 2252, 2252A, 2252B, or 2260 that involves child pornography; or

(B) section 1466A.

(b) **CONTENTS OF REPORT.—** To the extent the information is within the custody or control of an electronic communication service provider or a remote computing service provider, the facts and circumstances included in each report under subsection (a)(1) may include the following information:

(1) **Information about the involved individual.—** Information relating to the identity of any individual who appears to have violated a Federal law described in subsection (a)(2), which may, to the extent reasonably practicable, include the electronic mail address, Internet Protocol address, uniform resource locator, or any other identifying information, including self-reported identifying information.

(2) **Historical reference.—** Information relating to when and how a customer or subscriber of an electronic communication service or a remote computing service uploaded, transmitted, or received apparent child pornography or when and how apparent child pornography was reported to, or discovered by the electronic communication service provider or remote computing service provider, including a date and time stamp and time zone.

(3) **Geographic location information.—**

(A) **In general.—** Information relating to the geographic location of the involved individual or website, which may include the Internet Protocol address or verified billing address, or, if not reasonably available, at least 1 form of geographic identifying information, including area code or zip code.

(B) **Inclusion.—** The information described in subparagraph (A) may also include any geographic information provided to the electronic communication service or remote computing service by the customer or subscriber.

(4) **Images of apparent child pornography.—** Any image of apparent child pornography relating to the incident such report is regarding.

(5) **Complete communication.—** The complete communication containing any image of apparent child pornography, including—

(A) any data or information regarding the transmission of the communication; and

(B) any images, data, or other digital files contained in, or attached to, the communication.

CHILD PORNOGRAPHY IS DEFINED UNDER U.S. LAW AS THE VISUAL DEPICTION OF A MINOR ENGAGING IN SEXUALLY EXPLICIT CONDUCT.

18 USC § 2251
SEXUAL EXPLOITATION OF CHILDREN

(a) Any person who employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, or who transports any minor in or affecting interstate or foreign commerce, or in any Territory or Possession of the United States, with the intent that such minor engage in, any sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct, shall be punished as provided under subsection (e), if such person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

(b) Any parent, legal guardian, or person having custody or control of a minor who knowingly permits such minor to engage in, or to assist any other person to engage in, sexually explicit conduct for the purpose of producing any visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct shall be punished as provided under subsection (e) of this section, if such parent, legal guardian, or person knows or has reason to know that such visual depiction will be transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed, if that visual depiction was produced or transmitted using materials that have been mailed, shipped, or transported in or affecting interstate or foreign commerce by any means, including by computer, or if such visual depiction has actually been transported or transmitted using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce or mailed.

(c) (1) Any person who, in a circumstance described in paragraph (2), employs, uses, persuades, induces, entices, or coerces any minor to engage in, or who has a minor assist any other person to engage in, any sexually explicit conduct outside of the United States, its territories or possessions, for the purpose of producing any visual depiction of such conduct, shall be punished as provided under subsection (e).

(2) The circumstance referred to in paragraph (1) is that—
(A) the person intends such visual depiction to be transported to the United

States, its territories or possessions, by any means, including by using any means or facility of interstate or foreign commerce or mail; or

(B) the person transports such visual depiction to the United States, its territories or possessions, by any means, including by using any means or facility of interstate or foreign commerce or mail.

(d) (1) Any person who, in a circumstance described in paragraph (2), knowingly makes, prints, or publishes, or causes to be made, printed, or published, any notice or advertisement seeking or offering—

(A) to receive, exchange, buy, produce, display, distribute, or reproduce, any visual depiction, if the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct and such visual depiction is of such conduct; or

(B) participation in any act of sexually explicit conduct by or with any minor for the purpose of producing a visual depiction of such conduct; shall be punished as provided under subsection (e).

(2) The circumstance referred to in paragraph (1) is that—

(A) such person knows or has reason to know that such notice or advertisement will be transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mailed; or

(B) such notice or advertisement is transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means including by computer or mailed.

(e) Any individual who violates, or attempts or conspires to violate, this section shall be fined under this title and imprisoned not less than 15 years nor more than 30 years, but if such person has one prior conviction under this chapter, section 1591, chapter 71 section 1591, chapter 71, chapter 109A, or chapter 117, or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to aggravated sexual abuse, sexual abuse, abusive sexual contact involving a minor or ward, or sex trafficking of children, or the production, possession, receipt, mailing, sale, distribution, shipment, or transportation of child pornography, such person shall be fined under this title and imprisoned for not less than 25 years nor more than 50 years, but if such person has 2 or more prior convictions under this chapter, chapter 71, chapter 109A, or chapter 117, or under section 920 of title 10 (article 120 of the Uniform Code of Military Justice), or under the laws of any State relating to the sexual exploitation of children, such person shall be fined under this title and imprisoned not less than 35 years nor more than life. Any organization that violates, or attempts or conspires to violate, this section shall be fined under this title. Whoever, in the course of an offense under this section, engages in conduct that results in the death of a person, shall be punished by death or imprisoned for not less than 30 years or for life.

While this law defines child pornography as “depictions of a minor engaging in sexually explicit conduct,” the actual defining characteristics of a pornographic image are more subjective. Many court cases now use “Dost factors” (named after the case of U.S. v. Dost from 1986) to determine whether an image is pornographic. Dost factors ask a few critical questions that help distinguish child pornography from innocent “bathtub pictures” and other non-pornographic images.

From the Dost case, the guidelines are:

"...This Court feels that, in determining whether a visual depiction of a minor constitutes a "lascivious exhibition of the genitals or pubic area" under § 2255(2)(E), the trier of fact should look to the following factors, among any others that may be relevant in the particular case:

1) Whether the focal point of the visual depiction is on the child's genitalia or pubic area;

2) Whether the setting of the visual depiction is sexually suggestive, i.e., in a place or pose generally associated with sexual activity;

3) Whether the child is depicted in an unnatural pose, or in inappropriate attire, considering the age of the child;

4) Whether the child is fully or partially clothed, or nude;

5) Whether the visual depiction suggests sexual coyness or a willingness to engage in sexual activity;

6) Whether the visual depiction is intended or designed to elicit a sexual response in the viewer.

Of course, a visual depiction need not involve all of these factors to be a "lascivious exhibition of the genitals or pubic area." The determination will have to be made based on the overall content of the visual depiction, taking into account the age of the minor."
US. V. Dost, 1986

CHILD SEX TRAFFICKING

18 USC § 1591 - SEX TRAFFICKING OF CHILDREN OR BY FORCE, FRAUD, OR COERCION

(a) Whoever knowingly—

(1) in or affecting interstate or foreign commerce, or within the special maritime and territorial jurisdiction of the United States, recruits, entices, harbors, transports, provides, obtains, or maintains by any means a person; or

(2) benefits, financially or by receiving anything of value, from participation in a venture which has engaged in an act described in violation of paragraph (1), knowing, or in reckless disregard of the fact, that means of force, threats of force, fraud, coercion described in subsection (e)(2), or any combination of such means will be used to cause the person to engage in a commercial sex act, or that the person has not attained the age of 18 years and will be caused to engage in a commercial sex act, shall be punished as provided in subsection (b).

(b) The punishment for an offense under subsection (a) is—

(1) if the offense was effected by means of force, threats of force, fraud, or coercion described in subsection (e)(2), or by any combination of such means, or if the person recruited, enticed, harbored, transported, provided, or obtained had not attained the age of 14 years at the time of such offense, by a fine under this title and imprisonment for any term of years not less than 15 or for life; or

(2) if the offense was not so effected, and the person recruited, enticed, harbored, transported, provided, or obtained had attained the age of 14 years but had not attained the age of 18 years at the time of such offense, by a fine under this title and imprisonment for not less than 10 years or for life.

(c) In a prosecution under subsection (a)(1) in which the defendant had a reasonable opportunity to observe the person so recruited, enticed, harbored, transported, provided, obtained or maintained, the Government need not prove that the defendant knew that the person had not attained the age of 18 years.

(d) Whoever obstructs, attempts to obstruct, or in any way interferes with or prevents the enforcement of this section, shall be fined under this title, imprisoned for a term not to exceed 20 years, or both.

(e) In this section:

(1) The term "abuse or threatened abuse of law or legal process" means the use or threatened use of a law or legal process, whether administrative, civil, or criminal, in any manner or for any purpose for which the law was not designed, in order to exert pressure on another person to cause that person to take some action or refrain from taking some action.

(2) The term "coercion" means—

(A) threats of serious harm to or physical restraint against any person;

(B) any scheme, plan, or pattern intended to cause a person to believe that failure to perform an act would result in serious harm to or physical restraint against any person; or
(C) the abuse or threatened abuse of law or the legal process.

(3) The term "commercial sex act" means any sex act, on account of which anything of value is given to or received by any person.

(4) The term "serious harm" means any harm, whether physical or nonphysical, including psychological, financial, or reputational harm, that is sufficiently serious, under all the surrounding circumstances, to compel a reasonable person of the same background and in the same circumstances to perform or to continue performing commercial sexual activity in order to avoid incurring that harm.

(5) The term "venture" means any group of two or more individuals associated in fact, whether or not a legal entity.

CHILD SEX TOURISM

18 USC § 2423
TRANSPORTATION OF MINORS

(A) **TRANSPORTATION WITH INTENT TO ENGAGE IN CRIMINAL SEXUAL ACTIVITY**. — A person who knowingly transports an individual who has not attained the age of 18 years in interstate or foreign commerce, or in any commonwealth, territory or possession of the United States, with intent that the individual engage in prostitution, or in any sexual activity for which any person can be charged with a criminal offense, shall be fined under this title and imprisoned not less than 5 years and not more than 30 years.

(B) **TRAVEL WITH INTENT TO ENGAGE IN ILLICIT SEXUAL CONDUCT.** — A person who travels in interstate commerce or travels into the United States, or a United States citizen or an alien admitted for permanent residence in the United States who travels in foreign commerce, for the purpose of engaging in any illicit sexual conduct with another person shall be fined under this title or imprisoned not more than 30 years, or both.

(C) **ENGAGING IN ILLICIT SEXUAL CONDUCT IN FOREIGN PLACES.** — Any United States citizen or alien admitted for permanent residence who travels in foreign commerce, and engages in any illicit sexual conduct with another person shall be fined under this title or imprisoned not more than 30 years, or both.

(D) **ANCILLARY OFFENSES**. — Whoever, for the purpose of commercial advantage or private financial gain, arranges, induces, procures, or facilitates the travel of a person knowing that such a person is traveling in interstate commerce or foreign commerce for the purpose of engaging in illicit sexual conduct shall be fined under this title, imprisoned not more than 30 years, or both.

(E) **ATTEMPT AND CONSPIRACY**. — Whoever attempts or conspires to violate subsection (a), (b), (c), or (d) shall be punishable in the same manner as a completed violation of that subsection.

(F) **DEFINITION.** — As used in this section, the term "illicit sexual conduct" means (1) a sexual act (as defined in section 2246) with a person under 18 years of age that would be in violation of chapter 109A if the sexual act occurred in the special maritime and territorial jurisdiction of the United States; or (2) any commercial sex act (as defined in section 1591) with a person under 18 years of age.

(G) **DEFENSE.** — In a prosecution under this section based on illicit sexual conduct as defined in subsection (f)(2), it is a defense, which the defendant must establish by a preponderance of the evidence, that the defendant reasonably believed that the person with whom the defendant engaged in the commercial sex act had attained the age of 18 years.

APPENDIX B: RELEVANT EXAMPLES

EXAMPLE: ENCOURAGING USER SAFETY

Facebook worked with an organization called Connect Safely to create an informational guide for users who are feeling uncomfortable while engaging in online activity on their site.

A relationship on Facebook is making me uncomfortable. What should I do?

First, never agree to do anything that makes you feel uncomfortable. You're in charge of your life. Even if another person seems to be a friend, they're no friend if they're trying to get you to do anything against your will or your best interests.

It's hard to make a good decision when you're feeling confused, so you should be as clear as possible in your own mind about what is and isn't in your own interests. If you need help with this, talk to someone you trust.

- If you receive any unwanted sexual comments or communication on Facebook, the best thing you can do is remove yourself from the conversation. If it doesn't stop immediately, you should block the person and consider talking about it with an adult you trust and reporting it to Facebook.

- If you're under 18 and someone's putting pressure on you that's sex-related, don't hesitate to call the police or the CyberTipline at **1-800-843-5678**. They have advisers available 24/7 to help.

- If this person's a relative or someone in your household and you need help, contact the police, go to *https://ohl.rainn.org/online* or call the National Sexual Assault Hotline at **1-800-656-HOPE (4673)**.

For more information please visit *www.connectsafely.com/safety-advice-articles/how-to-recognize-grooming.*

OTHER RESOURCES

FAIR FUND BEST PRACTICES GUIDE:
http://www.prostitutionresearch.com/pdfs/BestPracticesGuideExploitationChildTraffickingFinal.pdf

GEEBO BEST PRACTICES GUIDE:
http://geebo.com/pages/view/id/5-social_responsibility/#Endorsements

INTERNET MERCHANT ACQUISITION BEST PRACTICES:
http://icmec.org/en_X1/pdf/InternetMerchantAcquisition.pdf

TECHNOLOGY COALITION WEBSITE:
http://technologycoalition.org

FINANCIAL COALITION AGAINST CHILD PORNOGRAPHY REPORT ON TRENDS IN ONLINE CRIME:
http://bit.ly/1oOHjLR

GSMA PREVENTING MOBILE PAYMENT FOR CHILD SEXUAL ABUSE CONTENT:
http://bit.ly/1q4oyYx

BEST PRACTICES FOR FILE HOSTING AND FILE SHARING COMPANIES:
http://bit.ly/TY0Fma

CONTACT:

Programs@wearethorn.org