THE TECHNOLOGY
COALITION

EMPLOYEE RESILIENCE GUIDEBOOK

FOR HANDLING

CHILD SEXUAL ABUSE IMAGES

January 2015 (Version Two)
http://technologycoalition.org

EMPLOYEE RESILIENCE GUIDEBOOK FOR HANDLING CHILD SEXUAL EXPLOITATION IMAGES

The Technology Coalition
January 2015 –Version Two

TABLE OF CONTENTS

INTRODUCTION

The Technology Coalition is powered by leaders in the Internet services sector. Formed in 2006, the Coalition's vision is to eradicate online child sexual exploitation. Its strategies are to:

- Sponsor the development of technology solutions that disrupt the ability to use the Internet to exploit children or distribute child pornography; and
- Seek and create platforms for collaboration between the private and public sectors for the creation of standards, and the sharing of best practices and similar initiatives that advance the fight against the online sexual exploitation of children.

The Technology Coalition works with the National Center for Missing & Exploited Children (NCMEC) and the International Centre for Missing & Exploited Children (ICMEC) to help identify and propagate technology solutions that create effective disruption. More information can be found at www.technologycoalition.org.

The members of the Technology Coalition are:

AOL Inc.
Facebook
Google Inc.
Microsoft Corporation
PayPal
Time Warner Cable
United Online, Inc.
Yahoo! Inc.

The Technology Coalition is funded by member companies and does not accept funding from any government agency or NCMEC.

Complying with laws against online child sexual exploitation is an important and potentially challenging responsibility for companies that offer Internet services. This resource's objective is to provide a high-level summary of an organization's obligations related to reporting apparent child sexual abuse material (CSAM) that may be on its systems. In addition, this resource offers a set of suggested practices and guidelines to support those employees who have exposure to online CSAM in the course of their work.

Organizations use a variety of names for initiatives to support employees in these functions including "Employee Wellness" and "Employee Safeguard" programs. The Technology Coalition has chosen to name this approach "Employee Resilience".

There are a variety of terms used to refer to images of child sexual exploitation. Throughout most of this paper, the term "child sexual abuse material" (CSAM) will be used.

This Guidebook was originally published in 2013. This second version has been updated and expanded.

DISCLAIMER

This Guidebook is intended to provide insight and high-level industry practices and is not intended to provide legal advice. The reader should consult with his or her legal team on what the company's obligations are in this area and whether or how it should implement these guidelines.

The specific practices and guidelines included in this document, which are offered in support of those employees who have exposure to online CSAM in the course of their work, are offered as samples for reference only and are not intended to represent the best or only approach to any particular issue. Neither the Technology Coalition nor any individuals or companies providing the practices or guidelines make any warranty or guarantee with regard to the accuracy, completeness or suitability of the practices and

guidelines, and they assume no responsibility or liability in connection with their use or misuse in a particular circumstance. The Technology Coalition makes no warranties, expressed, implied, or statutory, as to the information in this Guidebook.

LEGAL REPORTING AND OBLIGATIONS

Legal Definitions in the United States

Under federal law, Title 18 U.S.C. §2256, "child pornography" means any visual depiction of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Sexually explicit conduct includes graphic sexual intercourse, such as bestiality, masturbation, or sadistic or masochistic abuse. It also includes lascivious simulated sexual intercourse where the genitals, breast, or pubic area of any person is exhibited, or any graphic or simulated lascivious exhibition of the genitals or pubic area.

The National Center for Missing and Exploited Children® (NCMEC) has a summary of federal laws related to CSAM at http://www.missingkids.com/LegalResources/Exploitation/FederalLaw. Additional references on CSAM law can be found on the website of the Legal Information Institute at Cornell University at http://www.law.cornell.edu/.

Federal law, Title 18 U.S.C. §2258A, covers reporting requirements of electronic communication service providers and remote computing service providers.

Reporting to the National Center for Missing & Exploited Children

The National Center for Missing & Exploited Children (NCMEC) is a private, nonprofit organization that serves as the national clearinghouse and resource for the United States on the issues related to missing and sexually exploited children.

Under its Congressional designation, NCMEC operates the CyberTipline®, the national reporting mechanism concerning possible child sexual exploitation. It receives reports in eight categories:

- possession, manufacture, and distribution of CSAM;
- online enticement of children for sexual acts;
- child sex trafficking;
- sex tourism involving children;
- extra-familial child sexual molestation;
- unsolicited obscene material sent to a child;
- misleading domain names; and
- misleading words or digital images on the Internet.

These reports are made by electronic communication service providers and remote computing service providers, who are required by law to report apparent CSAM to the CyberTipline (18 U.S.C. §2258A). Members of the public also make reports to the CyberTipline. The CyberTipline (www.cybertipline.com; 1-800-843-5678) operates 24 hours a day and 7 days a week.

NCMEC analysts review and add value to the reports using publicly available search tools in an effort to determine a potential geographic location of the reported incident. NCMEC makes the CyberTipline reports available to the appropriate law enforcement agency for their independent review and potential investigation.

Providers of electronic communication services and remote computing services must make a report to NCMEC's CyberTipline when the provider has "actual knowledge of any facts and circumstances" of a violation of child sexual exploitation laws that involves apparent CSAM (e.g., the production, distribution, or possession of apparent CSAM; misleading domain names; and the obscene visual depiction of a minor). See 18 U.S.C. § 2251, 2251A, 2252, 2252A, 2252B, or 2260; 18 U.S.C. § 1466A, found at http://www.law.cornell.edu/uscode/text/18/2258A.

A company can report suspected child exploitation incidents to NCMEC via an online secure reporting form created specifically for this purpose. Companies can register with the CyberTipline by providing a mailing address, telephone number, facsimile number, and the electronic mail address of an individual point of contact at the company.

Companies wishing to register with the CyberTipline can contact NCMEC at espteam@ncmec.org. Once NCMEC has created an account for the company, it will send the company a link to the secure URL, along with a username and password. NCMEC also offers an XML Standard, referred to as its "Web Services" reporting system, for companies that prefer to automate reporting. Information about Web Services can be requested via the espteam@ncmec.org email account.

Information about the suspected incident that may be reported to NCMEC includes:

- Identifying information: Information about the involved user or customer, such as email address, IP address, or any other identifying information, including self-reported identifying information.

- Historical reference of the incident: This may include any information related to when and how the user or customer uploaded, transmitted, or received apparent CSAM, as well as when and how the material was reported or discovered, including the date, time stamp, and time zone.

- Geographic location of the user or website: IP address or verified billing address, or, if not available, area code, or zip code.

- Any images of apparent CSAM related to incident.

- Complete communication containing any image: This may include information on the transmission of the image or any other images, data, or files attached to or contained in the reported communication.

If the report is time-sensitive, both the manual reporting form and the Web Services reporting system offer companies the option of "escalating" the report, which will alert NCMEC to prioritize the report.

Statistics

As of October 2014, the CyberTipline has received more than 2.8 million reports of suspected child sexual exploitation since it was launched in 1998. Of the eight types of child sexual exploitation incidents that the CyberTipline receives, child pornography constitutes the vast majority of the reports.

Data Retention and Handling

Federal law, Title 18 U.S.C. §2258A, also requires that a company preserve the contents of its report for 90 days after NCMEC's receipt of the report. The company should preserve the contents of the report along with images, data, or other digital files that are commingled or interspersed among the reported images. Those materials must be kept in a secure location, which includes limiting access by employees to that material to the extent necessary to comply with the law.

Companies may also want to visit the website of the U.S. Internet Service Provider Association (USISPA) to review its "Industry Sound Practices for Reporting Apparent Child Pornography" (http://www.usispa.org/wp-content/uploads/2011/04/US-ISPA-Sound-Practices-Protect-Act.pdf).

SAFE HANDLING AND REPORTING PRACTICES

This section covers guidelines for developing safe handling and reporting practices. These guidelines are generalized and may not cover all of a company's reporting obligations. Coordination should take place among a company's legal, engineering, and other relevant teams to create a process that fulfills the organization's reporting obligations, as well as keeps data secure. Here are several safe handling and reporting guidelines based on industry practice:

1) Build tools to facilitate the reviewing and reporting process.

Limiting the amount of time employees are exposed to CSAM is key. NCMEC offers an automated reporting schema so that reports can be sent by XML rather than by filling out individual forms on the NCMEC system. Using this option, as well as developing other abuse-review tools, can significantly decrease the amount of time that an employee must spend reviewing CSAM. (The XML format additionally allows for more detailed and structured reporting.)

A company may want to consider utilizing industry-shared hashes to more easily detect and report CSAM and in turn, limit employee exposure to these images. Hash technology allows for identification of exactly the same image previously seen and identified as objectionable. To learn more contact NCMEC at espteam@ncmec.org.

Microsoft developed a hashing technology called PhotoDNA, which they have licensed to other companies in the industry through NCMEC. Companies interested in utilizing PhotoDNA can contact NCMEC at photodna@ncmec.org.

2) Build tools to ensure security in each step of compliance.

The servers that hold the CSAM should be secure and access to them should be limited to only the people involved in CSAM investigations. Consider providing a work space to the team that handles the CSAM investigation in an area that has little to no other traffic. In addition, consider providing employees with privacy screens for their monitors.

3) Create clear and well-documented policies and processes.

Sample policies that a company might consider include:

- Identifying specific individuals responsible for dealing with CSAM issues and requiring that they complete specific training.
- Requiring all employees handling CSAM to only do so from a corporate network.

- Establishing a Child Safety Team that ensures that all new products and services comply with the company's child safety policies and legal obligations. This team can be a standalone team or cross-functional team of representatives from relevant corporate functions.

4) Establish a well-informed team.

Before assigning CSAM investigations to an employee, be sure to get the employee's informed consent. This includes providing an appropriate level of information so the employee understands what the role entails without negatively impacting those who wouldn't want the job.

It is important that employees are pre-briefed before starting the job. Pre-briefing employees should include an in-depth description of the type of content they will be seeing and what warning signs they should be looking for in terms of their own possible negative reaction to the material. They should be informed of what company support resources are available to them. It is also recommended that these employees are interviewed in either one-on-one or group sessions, weekly, monthly, or quarterly so they can discuss their experiences in the job.

If the volume of material and company size warrant, a company should have a minimum of two people on the team investigating CSAM, in order to provide necessary backup for this function.

Many companies choose to centralize the team for CSAM investigations and reporting to limit the exposure to employees. This approach provides a more controlled environment.

Another option is to decentralize the function by expanding the responsibility of CSAM investigations across multiple teams and departments. While this increases exposure, the benefits include a more collaborative effort across multiple levels within the company so that there is emphasis on the importance of the role. In addition, it can promote a feeling of a company-wide commitment to combating the problem and more people can be involved cross-functionally in developing solutions.

5) Consider vendor policies.

If a company contracts with a third-party vendor to perform duties that may bring vendor employees in contact with CSAM, it is recommended that the contract with the vendor clearly outline requirements to keep the content secure, limit unnecessary exposure, and comply with all applicable laws, including those governing CSAM. Whenever possible, perform an initial audit of a contractor's wellness procedures for their employees.

6) Establish a feedback loop with NCMEC.

The knowledge that an employee's dedicated time and attention to this challenging task has resulted in rescuing children can be one of the most satisfying and motivating aspects of this job. There are several ways in which companies may learn about arrests and convictions of suspects as a result of their reports to NCMEC's CyberTipline.

NCMEC sends out a monthly bulletin to registered companies containing feedback on their reports that NCMEC has collected from law enforcement and news articles. The bulletin includes the report number, date of the report, location, report identifiers (i.e. email, username, and/or IP address), the status of the report (if it led to an arrest, conviction and/or sentence), and a published news article if one is available. Contact NCMEC at espteam@ncmec.org to place your company on the distribution list. Finally, local newspapers often publish stories about these cases. Set up an online alert that notifies you when articles appear with your company's name. You may see a story that describes the result of a report submitted by your team.

WHY FOCUS ON EMPLOYEE RESILIENCE?

A study conducted by the National Crime Squad in the United Kingdom reported that 76% of law enforcement officers surveyed reported feeling emotional distress in response to exposure to child abuse on the Internet. This same study, which was cosponsored by the U.K.'s Association of Chief Police Officers (ACPO), demonstrated the need for employee support programs to help them manage the traumatic effects of exposure to CSAM.

Recommendations from this study included:

- Having documented policies and procedures for staff viewing images of online child sexual exploitation and for identifying how this role and the individual should be managed;
- Maintaining open dialogue between managers and employees on the potential impacts and options for obtaining support;
- Creating transparent and robust hiring practices that adequately inform the potential employee of what type and how much potentially impactful content he/she will be exposed to; and
- Providing counseling services that are readily and easily available to all staff members who are exposed to CSAM.

In a more recent study, researchers analyzed 28 law enforcement officers and found that "greater exposure to disturbing media was related to higher levels of secondary traumatic stress disorder (STSD) and cynicism" and that "substantial percentages of investigators reported poor psychological well-being." (Source: http://www.kenwoodcenter.org/icac/documents/SecondaryTraumatic....pdf).

In 2007, psychologist Juliet Francis published "Helping the Helpers: Minimizing the Psychological Impact of Investigators Viewing Objectionable Material." In her study, she found that viewing CSAM in the course of an investigation could, "increase one's risk of exposure to the effects of secondary trauma," despite the professional and personal satisfaction the viewer may garner from having such a noble task of fighting against it. (Source: http://www.scribd.com/doc/24133366/Judith-AReisman-PhD-Picture-Poison).

This study notes that helpers may "have formed an empathetic engagement with a victim's trauma and as a result become vicariously traumatized." This can potentially result in "feelings of incompetence and hopelessness regarding one's abilities to help others, challenges to one's faith, a heightened sense of personal vulnerability, as well as distrust and cynicism about the human condition."

The same document points out that secondary trauma is associated with higher employee turnover, as well as increased employee sick leave and physical illness.

Employee morale and longevity are important issues for any organization and it is no different for the department that handles the reporting of apparent CSAM. The company and the function benefit by having staff members with the experience and knowledge to handle these functions efficiently.

THE HIRING PROCESS

Industries, such as law enforcement and emergency services, that require employees to be exposed to traumatic events or images have long understood the cause and effects of secondary trauma. Many have robust programs and policies to mitigate the impact on employees. The Internet industry has recognized that a similar approach should be considered for employees who are viewing CSAM.

The broader concept of Employee Resilience starts with the hiring process.

Whenever possible, these roles should be staffed voluntarily by employees who clearly understand the type of content to which they will be exposed.

Regardless of whether an employee has volunteered for a position or, out of necessity, has been placed in a position where exposure to potentially impactful content will occur, it is important to be transparent throughout the hiring process about the type of content to which he/she could potentially be exposed. Additionally, it is important to set realistic expectations about how much exposure employees can expect in their role. Some care needs to be taken to adequately prepare employees without traumatizing or overwhelming them before they even start in the position.

Some helpful resources to use when educating a candidate on what to expect include:

- The legal definition of child pornography, as codified in Title 18 U.S.C. §2256.
- National Center for Missing & Exploited Children (NCMEC) http://www.missingkids.com/home
- International Centre for Missing & Exploited Children (ICMEC) http://www.icmec.org/missingkids/servlet/PublicHomeServlet
- Internet Watch Foundation (IWF) (designated hotline for the U.K.) http://www.iwf.org.uk/http://www.iwf.org.uk/
- Child Exploitation and Online Protection Centre (CEOP)(law enforcement agency in the U.K. handling child sexual exploitation cases) http://ceop.police.uk/

A company should consider adjusting the level of transparency throughout the hiring process, based on the candidate's previous experience, comfort level and expected exposure level in the role. The following is an example of a possible hiring process transparency plan:

Informational Interview

- Use industry terms like "child sexual abuse imagery" and "online child sexual exploitation" to describe subject matter.
- Encourage candidate to go to websites (NCMEC, ICMEC, IWF, CEOP, etc.) to learn about the problem.

Follow-up Interviews

- Discuss candidate's previous experience/knowledge with this type of content.
- Discuss candidate's current level of comfort after learning more about the subject.
- Allow candidate to talk with employees who handle content about their experience, coping methods, etc. (Note: Caution employees to not disclose explicit examples of content.)
- Be sure to discuss any voluntary and/or mandatory counseling programs that will be provided if candidate is hired.

After Hiring

- Provide internal documentation on policies, content scenarios, etc., including an in-depth tutorial on applicable federal laws concerning CSAM. (Note: The legal definition of child pornography is explicit and detailed. New employees should be encouraged to make use of Employee Resilience services as needed.)
- In the first week of employment, perform a controlled content exposure with the new employee along with seasoned team members and/or a counseling service provider.
- Set up post-exposure counseling sessions for employee.

BUILDING AN EMPLOYEE RESILIENCE PROGRAM

If employees are going to be exposed to this type of content on a regular, ongoing basis as a function of their jobs, it is important for the company to have a robust, formal "resilience" program in place to support an employee's well-being and mitigate any effects of exposure.

Employee Resilience Programs should be tailored to fit the needs of the company and its team. There is no "one size fits all" program and program developers should investigate a range of program designs. Factors to consider when designing an Employee Resilience Program include: level of exposure, size of team, size of company, and available resources. Many companies have an Employee Assistance Program (EAP) that can be leveraged when developing individual safety plans and Employee Resilience Programs.

Measures to deal with incidental, or infrequent exposure to CSAM, should follow similar guidelines. If a non-designated employee has handled CSAM, it is important that she/he be given adequate access to the Employee Resilience Program.

Group support sessions can also be helpful on a monthly or quarterly basis. These sessions help employees understand that they are not alone in their feelings and that support is available to them.

While some employees may initially discount or disregard resources to help them cope with the potential impacts of this work, it is important for their managers to communicate the benefits of taking time away from the work and examining whether or not they need to take advantage of available resources.

Designing a tailored Employee Resilience Program is important. There are, however, certain elements that are critical to the success of any Employee Resilience Program.

- The program should include elements (e.g., education, intervention, counseling services, and evaluation) that are administered by a professional with specialized training in trauma intervention, ideally secondary trauma if the specialty is available.

- The professional care provider should be an outside resource, not an employee of the company. This ensures confidentiality and helps remove barriers to open communication.

Strong consideration should be given to making select elements of the program (such as counseling) mandatory for exposed employees. This removes any stigma for employees who want to seek help and can increase employee awareness of the subtle, cumulative effects that regular exposure may produce.

Following are two examples of possible Employee Resilience Programs:

Company A: Small Electronic Service Provider (ESP) that employs 300; handles a few child exploitative issues per month.	**Company B:** Large ESP and Social Networking services provider that employs 50,000; handles 50+ child exploitative issues per day.
Designate and train employees as warranted to handle issues.	Designate and train a centralized team to handle issues.
Develop shared workload plan, if warranted, so that no one person handles all apparent CSAM.	Develop shared workload plan, so that no one person handles all apparent CSAM.
Provide bi-annual education on the effects of exposure for employees (including supervisors), conducted by a professional specializing in secondary traumatic stress.	Provide mandatory monthly group counseling sessions for team.
Provide professional assistance in developing individual safety plans.	Provide mandatory quarterly individual counseling sessions for team members.
Provide access to emergency counseling services as needed by employees experiencing severe response.	Provide access to emergency counseling services as needed by employees experiencing severe response. Provide professional assistance in developing individual safety plans.
	Provide bi-annual education on the effects of exposure for employees (including supervisors), conducted by a professional specializing in secondary traumatic stress.

If your company contracts with vendors to perform online safety functions, consider using vendors that provide Employee Resilience Programs for their employees who handle CSAM as a regular part of their contracted duties.

PROMOTING "SELF CARE"

Another important principle that has been emphasized by professionals dealing with exposure to CSAM is a focus on self-care, including both long-term stress reduction techniques and immediate coping plans in the case of traumatic exposure.

Long-term stress reduction refers to typical "wellness" activities and includes concepts like exercise, healthy diet, adequate sleep, and good work-life balance. These are well understood and widely-accepted concepts, so this document will not go into detail except to reiterate the importance of a healthy, balanced lifestyle to combat the potential emotional impacts of long-term exposure.

Employees at risk for exposure to potentially traumatic content should have a personal plan to help them cope with any immediate trauma responses. Having a personal safety plan to manage these responses may enable the employee to continue working on a critical project and could help mitigate the cumulative effects of repeated exposure.

It is important to note that a secondary traumatic stress response can occur after just one exposure to impactful content. Traumatic responses may include immediate or delayed expressions of grief or anger, a heightened sense of personal vulnerability, intrusive thoughts and difficulty sleeping. These can result in reduced productivity on the job, an increase in lateness and absenteeism, job avoidance, interpersonal conflict, and increased expressions of anger.

Keep in mind that while this document addresses CSAM, employees can also be impacted by other types of content, such as violence against people or animals.

Safety plans should be tailored to the individual. While there are various support resources available to help an employee develop his or her safety plan (e.g., managers, human resources, fellow employees), it is strongly recommended that safety plans be developed with assistance from a professional counselor who is trained in secondary traumatic stress.

Below is a sample safety plan. It includes a variety of activities that an employee may use depending on the depth of his or her reaction.

- Go for a 15-minute walk outside - not on "auto pilot" - but in a manner which is mindfully aware. Mindfulness is a necessary component of any stress reduction activity.
- Talk to a friend. (Designate specific person(s) and get consent from them ahead of time.) Ask colleagues about different ways of discussing one's work (this has been identified as a particular barrier as people unfamiliar with the work cannot relate to the content or may have a negative reaction to what they are hearing).
- Attend on-site group and individual wellness sessions, if available.
- Research and understand the physiological basis of the stress response to support greater productivity and to gain an understanding of how stress reduction works.
- Practice stress reduction activities during the work day. These may include building an awareness of your body's physical reactions to stress, breath control, and sensory integration exercises.
- Be aware of personal stress indicators and triggers so early intervention can be sought/implemented. Be aware of subtle changes in your behavior that can indicate the build-up of stress.
- Identify the value of the work on a personal, professional, and societal basis. If a person feels his or her work has meaning, it becomes easier to contextualize and tolerate its more difficult aspects.
- Do a different work activity for an hour.
- Go home. (Requires pre-planning and open dialogue with manager.)
- Participate in a team or group activity outside of work.

- Engage in a hobby or in a physical activity requiring concentration.
- Call counselor. (This could be an Employee Assistance Program, public hotline, or personal care provider.)
- Take time off. (Discuss this with a manager or supervisor.)

Connections with mental health professionals can increase the quality of a wellness program. These professionals can both help shape the program, as well as be an asset to the employees exposed to the content.

Companies should consider training the managers of these staff members to identify the signs and symptoms of secondary trauma and to outline what steps to take if a staff member is exhibiting secondary trauma. Managers should be encouraged to participate in self-care activities as well.

Opting-out Procedures

Having clear opt-out mechanisms available is another important facet of a wellness regime. When possible, before employees begin their work, provide clear guidelines for how and when they may remove themselves from the work. The opt-out communication between employee and supervisor should be confidential. The time allowed away from the work should be communicated to the employee from the start. The duration of the break should be decided on a case-by-case basis.

Below are examples of opt-out reasons:

- Close relationship to someone who has experienced sexual assault
- Anxiety related to the work
- Depression

CONCLUSION

Responsible members of the Internet industry are actively meeting their obligations to report apparent CSAM on their systems in order for NCMEC, law enforcement, and others to pursue the appropriate actions to help keep children safe. In addition to developing technology tools, the industry recognizes that it must support those employees who are on the front lines of this battle. It is the hope of the Technology Coalition that this Guidebook and suggested resources enhance those efforts.

ADDITIONAL RESOURCES

The U.K.-based Child Exploitation and Online Protection Centre – background on problems and solutions: http://ceop.police.uk/

Enough is Enough – statistics on child sexual exploitation:
http://www.enough.org/inside.php?tag=statistics#3

Internet Watch Foundation – the U.K. hotline for reporting suspected child sexual abuse:
http://www.iwf.org.uk/

Study on "Secondary Traumatic Stress and Burnout among Law Enforcement Investigators Exposed to Disturbing Media Images:"
http://www.kenwoodcenter.org/icac/documents/SecondaryTraumatic....pdf

U.S. reporting requirements of electronic communication service providers and remote computing service providers: http://www.law.cornell.edu/uscode/text/18/2258A

National Center for Missing & Exploited Children (NCMEC):
http://www.missingkids.com/Home

NCMEC Key Facts and CyberTipline Fact Sheet: http://www.missingkids.com/KeyFacts
http://www.missingkids.com/en_US/documents/PressKit_Cybertipline.pdf

NCMEC's CyberTipline – How to Submit a Report:
http://www.missingkids.com/CyberTipline

U.S. federal laws concerning the sexual exploitation of children:
http://www.missingkids.com/LegalResources/Exploitation/FederalLaw

International Centre for Missing & Exploited Children (ICMEC)
http://www.icmec.org/missingkids/servlet/PublicHomeServlet

National District Attorneys Association, National Center for Prosecution of Child Abuse-U.S. state statutes: http://www.ndaa.org/ncpca_state_statutes.html

Article about the "Helping the Helpers" study:
http://www.scribd.com/doc/24133366/Judith-AReisman-PhD-Picture-Poison

The Technology Coalition's website: http://technologycoalition.org/ and "Projects" page
http://technologycoalition.org/coalition-projects/

Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings from the *National Juvenile Online Victimization Study:*
http://www.unh.edu/ccrc/pdf/jvq/CV81.pdf

Crimes Against Children Research Center – "Work Exposure to Child Pornography in ICAC Task Forces and Affiliates": http://unh.edu/ccrc/pdf/Law%20Enforcement%20Work%20Exposure%20to%20CP.pdf

U.S. Internet Service Provider Association, Industry Sound Practices for Reporting Apparent Child Pornography: http://www.usispa.org/wp-content/uploads/2011/04/US-ISPA-Sound-Practices-Protect-Act.pdf

# # #