Confronting New Challenges in the Fight Against Child Pornography:

Considerations for Protecting Children & Your Company's Reputation When Engaging with Digital Businesses

January 2014

International Centre
FOR MISSING & EXPLOITED CHILDREN

TABLE OF CONTENTS

ACKNOWLEDGMENTS

The International Centre for Missing & Exploited Children (ICMEC) wishes to thank the following organizations and individuals for their contributions to this paper:

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

ICMEC gratefully acknowledges the support of PayPal in the development of this paper.

DISCLAIMER

This report ("Report") was created and written by volunteers on behalf of ICMEC and represents the current views of the issues addressed as of the date of publication. The content of the Report is based on the individual input of the contributors and does not necessarily reflect the opinions or policies of the companies at which the individuals work. There may be inaccuracies or information that has become outdated since this Report was originally written.

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

INTRODUCTION

The International Centre for Missing & Exploited Children (ICMEC) is a leading global service agency working to protect children from sexual abuse, exploitation, and abduction.[1] ICMEC strongly believes that global advertisers, financial institutions, payment processors, credit card companies, and hosting companies must have confidence that their platforms, products, and institutions are not unintentionally providing financial support to, or otherwise legitimizing, "rogue" Internet sites which allow for the distribution and/or storage of child pornography. As well, these industry groups must have confidence that their corporate brands and images are not being harmed by association with such unlawful activity.

Digital business models on the Internet present specific challenges in the fight against online child sexual exploitation content. As the e-commerce ecosystem broadens, numerous industry sectors are looking for guidance on how to engage with partners in the digital world in a manner that allows for the protection of children and their company's reputation.

ICMEC launched an initiative as part of its Asia Pacific Financial Coalition's Technology Challenges Working Group to support a variety of enterprises in the prevention and detection of online child sexual abuse material, by sharing industry best practices.

The goal of this paper is to help companies manage risk and relationships by providing information on the digital platforms/business models that can be abused for the purpose of distributing child sexual exploitation content.

The first phase of this project addresses the following business models:

- BitTorrent
- File Sharing Providers
- Massively Multiplayer Online Role Playing Games (MMORPGs), such as Second Life
- Newsgroups
- Social Media

The summary for each business model includes a description of how the platform works as well as references to how it has been or might be used for the storage and/or distribution of child pornography. The last section of the paper outlines risk management practices to consider when doing business with these types of companies.

The second phase of this project will address additional digital business models such as live video streaming and Internet Relay Chat (IRC).

[1] To learn more visit www.icmec.org.

DIGITAL BUSINESS MODEL SUMMARIES

BitTorrent

BitTorrent provides a platform for transferring large files and large amounts of data over the Internet. First released in 2001, the total number of active monthly users on BitTorrent is estimated to be more than a quarter of a billion.[2] The company behind the technology, BitTorrent Inc., was founded in 2004 to monetize the service. BitTorrent is an example of peer-to-peer file sharing, which means that instead of downloading a file from a single source, like iTunes, users download fragmented files from other users.[3] By downloading multiple pieces at the same time, the overall speed is greatly improved. The more computers involved, the faster the file transfer occurs. A number of academic institutions and companies use BitTorrent to distribute large files.

BitTorrent software is free to download and many versions of the software are open source. The company itself generates revenue through advertising, search inventory syndication, and by licensing its own version of the protocol to consumer electronics companies, which can then embed the technology in everything from televisions to smartphones.[4]

Some sites encourage users to make donations, usually facilitated by online payment service providers. Numerous venture capital firms have funded BitTorrent operations.

Relevance to the Fight Against Child Pornography

BitTorrent software poses a particular problem for stopping the trade of illicit images because it breaks the files into pieces and sends them from one computer to the next via different paths without passing through any centralized servers. Child predators can share images, videos, or other content by first creating a small descriptor file, or "torrent," that can be distributed via the Web or e-mail. The torrent file will tell anyone interested in downloading this content how to contact a "tracker" computer that coordinates the matching of consumers with suppliers. Because of the way BitTorrent works, the consumer ultimately receives different pieces of content from multiple computers with different IP (Internet Protocol) addresses.[5]

In 2011, Computer Law & Security Review published an article titled *Internet Subcultures and Pathways to the Use of Child Pornography*. The article focused on isoHunt, which calls itself the most advanced BitTorrent search engine, and analyzed the child pornography search terms that consistently appeared in the isoHunt "Top 300 Search Terms" over a three month period. The article stated "Child pornography search terms ranked ahead of popular films, such as Harry Potter, common pornography terms, such as 'amateur', and software downloads such as 'Microsoft Office'".[6]

[2] Timothy B. McCormack, *The Evolution of BitTorrent's Legality*, seattlepi.com, 26 July 2013, *at* http://blog.seattlepi.com/timothymccormack/2013/07/26/the-evolution-of-bittorrents-legality/?shared=email&msg=fail (last visited 6 January 2014).

[3] Matt Hartley, *BitTorrent Turns Ten*, Financial Post, 1 July 2011, *at* http://business.financialpost.com/2011/07/01/bittorrent-turns-ten/?__lsa=885f-9d6a (last visited 2 January 2014).

[4] *Id.*

[5] Larry Greenemeier, *Cops Enlist Data-Tracking Software in the Fight against Child Predators*, Scientific American, 7 November 2011, *at* http://www.scientificamerican.com/article.cfm?id=software-against-p2p-bittorrent-abuse (last visited 2 January 2014).

[6] Jeremy Prichard, Paul Watters, and Caroline Spiranovic, *Internet subcultures and pathways to the use of child pornography*, Computer Law & Security Review, December 2011, Vol. 27, Issue 6, 585-600.

File Sharing Providers

File sharing sites allow users to upload content that can be accessed by other individuals through the same user account or by being given access credentials to view the content.

Terminology regularly associated with and/or used in place of file sharing sites includes, cyberlockers, cloud storage, file hosting services, and peer-to-peer (P2P) platforms/exchanges.

Under the traditional Internet client/server model, the access to information and services is accomplished by the interaction between users (clients) and servers—usually Web sites or portals. A client is defined as a requester of services, and a server is defined as the provider of services. Unlike the traditional model, the peer-to-peer model enables consenting users—or peers—to directly interact and share information with each other without the intervention of a server. A common characteristic of peer-to-peer programs is that they build virtual networks with their own mechanisms for routing message traffic.[7]

One type of file sharing site is a cyberlocker. Cyberlockers are third-party file sharing services, also known as "file hosting" services. The links to content are then made available to be searched either directly through search engines or through indexing sites. Such content can then be downloaded from the cyberlocker.

Some file sharing sites provide their services for free; others generate income by offering enhanced services for a fee, charging regular subscription fees, and/or generating revenue by selling advertisement space on the site.

Relevance to the Fight Against Child Pornography

The decentralized nature of the Internet, and resultant difficulties in restricting the distribution of child pornography, is exemplified by file sharing sites involving direct connections between computers without the need for centralized servers.[8]

In the fight against child pornography, much attention has been focused on peer-to-peer platforms, within the broader file sharing category. According to the *Threat Assessment of Child Sexual Exploitation and Abuse*[9] produced in 2012 by the U.K.'s Child Exploitation and Online Protection Centre (CEOP), peer-to-peer networking or file sharing is one of the principal routes for the distribution of this type of illegal content.

The CEOP report continues with the following observations:

> These systems are developing to create a relatively enclosed global network environment for the distribution of indecent images of children in both still and video form. A key characteristic of a new generation of P2P, which sets it apart from conventional facilities,

[7] U.S. General Accounting Office (GAO), *File-sharing Programs: Peer-to-Peer Networks Provide Ready Access to Child Pornography*, February 2003, *at* http://www.gao.gov/new.items/d03351.pdf (last visited 2 January 2014).

[8] Richard Wortley and Stephen Smallbone, *Child Pornography on the Internet*, Community Oriented Policing Services (COPS) No. 41, May 2012, *at* http://www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf (last visited 2 January 2014).

[9] U.K. Child Exploitation and Online Protection Centre (CEOP), *Threat Assessment of Child Sexual Exploitation and Abuse* 11, 2012, *at* http://www.ceop.police.uk/Documents/ceopdocs/CEOPThreatA_2012_190612_web.pdf (last visited 2 January 2014).

> is that in order to share files, users must first be invited into smaller groups in much the same way as happens in social networking environments. This means that it is not possible for those outside the group to see which files are available from a particular user. CEOP is aware of a number of international investigations that have focused on such P2P services which have resulted in successful prosecutions.

In its *2011 Annual Report*,[10] the Internet Watch Foundation (IWF) noted that over the previous two years it has seen an increasing number of legitimate websites being criminally exploited to host child sexual abuse content. The IWF also reported that image hosting sites (also known as weblockers, cyberlockers, or one-click hosting) are the mostly likely to be abused with 45% of the reported child sexual abuse content found on those types of sites.

Massively Multiplayer Online Role-Playing Games (MMORPGs)

Massively Multiplayer Online Role-Playing Games (MMORPGs), are computer-based role-playing games (RPG), which take place in an online virtual world with hundreds or thousands of other players. In the game, a player uses a client to connect to a server, usually run by the publisher of the game, which hosts the virtual world and collects information about the player.[11]

Even when a player is logged off of the game, events are occurring across the world that may impact the player when he/she logs in again. MMORPGs most often contain tools that facilitate communication between players, such as chat and instant messaging.

MMORPGs utilize a wide range of business models to generate funding. These business models include:

- **Free-to-play**: The consumer may pay to purchase software but there is no subscription charge or additional payments needed to access game content.
- **Pay-to-play**: Players must pay, usually by monthly subscription, in order to participate in the game.
- **Freemium**: The majority of game content is available for free, but players can pay for extra content or added perks.
- **Advertising:** Some games provide companies with the opportunity to pay to advertise on the sites.

Relevance to the Fight Against Child Pornography

MMORPGs offer the ability to customize one's experience, create avatars, join chat rooms online, as well as upload and share content. All of these tools can increase the risk of viewing and distributing child pornography within the site/game.

Each gaming platform has some form of storage capacity and, much like a traditional personal computer, can be used for storing pictures and videos. This provides a child pornographer with another method to

[10] Internet Watch Foundation (IWF), 2011 Annual and Charity Report 15, *at* https://www.iwf.org.uk/assets/media/annual-reports/annual%20med%20res.pdf (last visited 2 January 2014).

[11] What is a MMORPG?, 25 December 2013, *at* http://www.wisegeek.com (last visited 3 January 2014).

hide illicit images. The file sharing permitted by these systems and embedded into virtual worlds and online gaming communities offer new potential distribution mechanisms for these illegal materials.[12]

British police are going undercover in Second Life (an MMORPG) to investigate depictions of adult-child sex to track down pedophiles. Users, parents and, increasingly, lawmakers are concerned that platform providers reserve the right to set the rules, to collect and utilize user data and to self-police (or not). They worry about what goes on inside virtual worlds, including virtual child pornography.[13]

Newsgroups

A newsgroup is a continuous public discussion about a particular topic. A person can join a newsgroup at any time to become part of a huge conversation between hundreds or even thousands of people. Newsgroups are decentralized, which means that the messages are not maintained on a single server, but are replicated to hundreds of servers around the world.[14] In order to connect with a newsgroup, you need a newsreader, also referred to as a Usenet browser. Usenet is an Internet discussion forum distributed worldwide that has been in existence for over 30 years.[15]

Usenet newsgroups are hosted by a diverse collective, including Internet Service Providers, universities, and private businesses. Although there are a large number of newsgroup hosts, most have arrangements to keep their servers in sync, so that any user can find data posted by any other user, regardless of their particular host. Usenet newsgroups are considered networks because of the sharing of content between Usenet hosts.[16]

Many Usenet services charge for access – these are called payservers. Some payservers offer monthly subscriptions, and/or charge fees for premium services such as having a large number of connections, increased amounts of online storage, and other factors. Selling advertisement space on the site and/or requiring consumers to pay for each download provide additional channels for generating revenue.

Relevance to the Fight Against Child Pornography

The *Problem-Oriented Guides for Police,* published by the U.S. Department of Justice, address many criminal activities. The May 2010 issue that focuses on child pornography online provides the following information about newsgroups:[17]

> Specific child pornography newsgroups provide members with a forum in which to discuss their sexual interests in children and to post child pornography. This is one of the major methods of distributing child pornography. Some child pornography newsgroups are well known to both users and authorities. Most commercial servers block access to

[12] International Association of Chiefs of Police, IACP Center for Social Media, *Real Crimes in Virtual Worlds*, March 2012, page 4, *at* http://www.iacpsocialmedia.org/Portals/1/documents/External/Drakontas%20Real%20Crimes%20in%20Virtual%20Worlds.pdf (last visited 25 January 2014).

[13] M.M. White & B.L. Mann, *Blurring our real and virtual worlds: Canadian and worldwide legal issues arising from MMORPGs*, 14 June 2009, page 9.

[14] How Newsgroups Work, 2013, *at* http://www.howstuffworks.com (last visited 3 January 2014).

[15] What is Usenet?, 2013, *at* http://www.usenet.org (last visited 3 January 2014).

[16] Usenet and Newsgroups: What is Usenet?, *at* http://www.giganews.com/usenet.html (last visited 25 January 2014*)*.

[17] *Child Pornography on the Internet*, *supra* note 8.

> such sites. Some servers do provide access to them, but a user runs the risk of having his/her identity captured either by the credit card payments required for access, or the record kept by the server of his/her IP address. However, a computer-savvy user can access these groups by using techniques that hide his/her identity by concealing his/her true IP address.

According to the Internet Watch Foundation, only the more radical elements of Usenet are consistently abused, many of which can be found under the alt.* hierarchy.[18] The alt.*hierarchy is an alternative to the mainstream newsgroups. It was formed by people who wanted to create groups without having to go through discussion or votes with other group members.[19]

In 2008, Verizon Communications, Time Warner Cable, and Sprint Nextel signed an agreement with then Attorney General of New York, Andrew Cuomo, to shut down access to sources of child pornography. Time Warner Cable stopped offering access to Usenet; Verizon's plan was to eliminate some "fairly broad newsgroup areas", and Sprint said it would no longer offer any of the tens of thousands of alt.* Usenet newsgroups.[20]

In October 2013, the European Financial Coalition against Commercial Sexual Exploitation of Children Online published *The Commercial Sexual Exploitation of Children Online: A Strategic Assessment*.[21] The report made the following observations about newsgroups:

> Contrary to expectations that they would be entirely superseded by more recent social services, bulletin boards (BBS), newsgroups and IRC (Internet Relay Chat) remain in use. It is thought that some offenders may see greater security in continuing to use a trusted platform and view newer untested services with suspicion.

Social Media

Social media sites employ mobile and web-based technologies to create highly interactive platforms via which individuals and communities share, co-create, discuss, and modify user-generated content.[22]

There are many platforms that fall under the social media umbrella. Two researchers classified six different types of social media: collaborative projects (e.g., Wikipedia); blogs and microblogs (e.g., Twitter); content communities (e.g., YouTube); social networking sites (e.g., Facebook); virtual game worlds (e.g., World of Warcraft); and virtual social worlds (e.g., Second Life).[23]

[18] Email sent to ICMEC by Fred Langford, Director of Global Operations, Internet Watch Foundation, 15 October 2013.

[19] David Barr, The Pennsylvania State University, *So You Want to Create an Alt Newsgroup*, http://www.faqs.org/faqs/alt-creation-guide/ (last visited 14 January 2014).

[20] Declan McCullagh, *N.Y. Attorney General Forces ISPs to Curb Usenet Access*, CNET News, 10 June 2008, http://news.cnet.com/8301-13578_3-9964895-38.html (last visited 17 January 2014).

[21] European Financial Coalition against Commercial Sexual Exploitation of Children Online, *Commercial Sexual Exploitation of Children Online: A Strategic Assessment*, October 2013, *at* http://www.europeanfinancialcoalition.eu/private10/images/document/5.pdf (last visited 3 January 2014).

[22] Jan H. Kietzmann, Kristopher Hermkens, Ian P. McCarthy, Bruno S. Silvestre, *Social media? Get Serious! Understanding the functional building blocks of social media*. Business Horizons, Vol. 54, Issue 3, May-June 2011, pages 241-251.

[23] Andreas M. Kaplan and Michael Haenlein, *Users of the world, unite! The challenges and opportunities of social media*, Business Horizons, Vol. 53, Issue 1, January-February 2010, pages 59-68.

Social media organizations are funded through several methods:

- **Advertising**: Organizations pay to advertise on the site.
- **Web Applications**: Sites collect a portion of the revenue generated from web applications used on their platform.
- **Affiliates:** Sites can earn revenue by posting affiliate links on their pages.
- **Premium Services**: Customers pay for add-ons and premium services.
- **Venture Capital**: Sites seek investment funds from venture capital firms.

Relevance to the Fight Against Child Pornography

Social media is not only a concern in the fight against the distribution of child pornography, but also as it relates to online enticement (grooming) of young people. CEOP's *Threat Assessment of Child Sexual Exploitation and Abuse* (2012), noted the following about online enticement:[24]

> Whilst children can make themselves vulnerable in relation to their online behaviour it is equally the case that offenders target and exploit this vulnerability. CEOP sees frequent grooming behaviour targeted towards children and social networking sites are the most commonly reported environment in which this activity takes place. This is likely to be due to the ease with which individuals can create profiles on such sites. Criminals use a number of methods to build friendships with children on social networking sites. Once a relationship is formed the offender will use their position to initiate some form of sexually exploitative activity, be that in non-contact forms via webcam or through contact offline.
>
> In some cases children are being abused to order by members of forums with the resulting imagery subsequently shared within the community. In due course, some of these first generation images and videos find their way onto peer-to-peer ('P2P'), image hosting and social networking sites on the open internet.

In 2011, a senior official in the U.S. Department of Justice described this case during a Congressional hearing.[25]

> In one ongoing case being investigated by the Criminal Division's Child Exploitation and Obscenity Section working with the Federal Bureau of Investigation and Immigration and Customs Enforcement, we are seeking to identify members of online groups using social networking sites to upload and trade images of the sexual abuse of children. One U.S. target of this investigation uploaded child sexual abuse images hundreds of times to several different groups of like-minded offenders – including one group that had thousands of members.

[24] *Threat Assessment of Child Sexual Exploitation and Abuse, supra* note 9, at 7.

[25] Data Retention as a Tool for Investigating Internet Child Pornography and Other Internet Crimes, A Statement of John Weinstein, Deputy Assistant Attorney Criminal Division, Before the Committee on Judiciary Subcommittee on Crime, Terrorism and Homeland Security, United States House of Representatives, 21 January 2011, *at* http://www.justice.gov/ola/testimony/112-1/01-25-11-crm-weinstein-testimony-re-data-retention-as-a-tool-for-investigating-internet-child-pornography-and-other-internet-crimes.pdf (last visited 3 January 2014).

CEOP, in its 2013 *Threat Assessment of Child Sexual Exploitation and Abuse*, observed the following: Where it could be determined from the reports of online child sexual exploitation, the most common offending environment was social networking at 48.5%.[26]

In 2013, media stories noted that the website Pinterest, a content sharing service, had reported child pornography images on its site to the National Center for Missing & Exploited Children (NCMEC) "We were incredibly surprised," said Utah Internet Crimes Against Children task force field commander Patty Reed. "We all thought Pinterest was a place to go post your recipes or decorating ideas. So we were incredibly surprised to find out people were also using it to pin child pornography and share child pornography."[27]

[26] U.K. Child Exploitation and Online Protection Centre (CEOP), *Threat Assessment of Child Sexual Exploitation and Abuse* 11, 2013, *at* http://www.ceop.police.uk/Documents/ceopdocs/CEOP_TACSEA2013_240613%20FINAL.pdf (last visited 2 January 2014).

[27] Pat Reavy, *Utah Investigating Child Pornography Posted on Pinterest*, Deseret News, 30 May 2013, *at* http://www.deseretnews.com/article/865580915/Utah-investigating-child-pornography-posted-on-Pinterest.html?pg=all (last visited 17 January 2014).

General Risk Management Practices

As noted earlier, digital business models on the Internet present specific challenges in the fight against child pornography. Numerous industry sectors are looking for guidance on how to engage with partners in the digital world in a manner that allows for the protection of children and their company's reputation. The following section outlines risk management practices to consider when doing business with digital enterprises.

One of the most effective ways to avoid engaging in a business relationship with a risky service provider is to screen sites and site owners prior to formalizing the relationship. This can include:

- Internet searches of the business' background, phone number, address, "doing/business/as" info (d/b/a), and email address.
- Identifying and researching all owners of the business.
- Identifying all aspects of the business:
    - What they sell
    - How they sell it
    - How they take care of the customer

Any site or owner that has been associated with illegal activity should be further reviewed and vetted against a company's risk tolerance policy.

In addition to the initial review, companies should arrange for a periodic review of all sites with which it has a business relationship, as well as the owners of those companies. This will help to identify any sites/individuals that might have become involved in illegal activities following the original engagement.

A company may also want to consider hiring a third party to either supply a list of sites that have been noted as engaging in illegal activity or screen clients and site relationships for suspicious behavior/content. This can be done for existing as well as new relationships.

All businesses should ensure that each site with which they do business has strong Terms and Conditions that prohibit the uploading and distribution of child pornography. It is essential to inquire how the company monitors and responds to reports of violating content and whether it has established a formal reporting process and a protocol for addressing these reports.

In March 2013, the Thorn Foundation published its *Sound Practices Guide to Fight Child Sexual Exploitation Online.*[28] One of the suggestions presented in the guide is for companies to encourage "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."

[28] Sound Practices Guide to Fight Child Sexual Exploitation Online, Thorn Foundation, *at* http://www.wearethorn.org/our-work-to-stop-child-trafficking-now/ (last visited 3 January 2014).

Risk Management Practices When Engaging With BitTorrent

In addition to the points above, the following is important if a company plans to engage with a BitTorrent provider. BitTorrent providers usually fall into two different categories: Software providers and Tracker Link Forums.

BitTorrent Software merchants provide the software that enables users to create/download/upload BitTorrent files. These software providers do not usually require an intense level of scrutiny as they are providing a tool and do not control what type of content is disseminated via their software.

Tracker Link Forums are a venue for BitTorrent users to publish tracker files that enable the download of BitTorrent files. Revenue is generally derived from donations and/or subscriptions that grant access to premium/VIP areas.

When considering doing business with a Tracker Link Forum, a company should require that the Tracker Link Forum monitor and respond to reports of violating content. This includes the establishment of a formal reporting process and a protocol for addressing these reports.

In addition, the Tracker Link Forum should establish standards to authenticate users in order to prevent repeat violations by previously expelled users who attempt to re-enter the forum via falsified information.

Risk Management Practices When Engaging With File Sharing Providers

File sharing sites may be legitimate, however, the following characteristics are sometimes associated with illegitimate business models and should be treated with extra scrutiny:

1. "Rewards," cash payments, or other incentives are paid to uploaders based on the number of times their files are downloaded or streamed.
2. Links to prohibited content are indexed or distributed on third party websites.
3. Free access to stored files may be limited by increased wait times, bandwidth throttling, download limits, captchas, online advertising, or other techniques to encourage the purchase of "premium" memberships.
4. Files are deleted unless the uploader purchases a "premium" membership or a file is regularly accessed.
5. The site provides a "link checker", which allows uploaders to check whether a link has been disabled to facilitate re-upload of content removed.
6. The site provides uploaders with "forum codes" and "URL codes" to facilitate incorporation of the links on third party indexing or "linking" websites.

Risk Management Practices When Engaging With Newsgroups

The Internet Watch Foundation maintains a list of banned newsgroups and those that Usenet providers are recommended not to run due to the amount of illegal material that has been hosted within them over a set period of time. The IWF also provides a posting notice and takedown service for IWF industry members to remove illegal posts made into groups less frequently abused.[29]

[29] For additional information about IWF's programs visit https://www.iwf.org.uk/.

CONCLUSION

The digital marketplace offers a vast array of exciting business opportunities and marketing tools. However, a company **does not want to unintentionally provide financial support to, or otherwise legitimize, "rogue" Internet sites, which allow for the distribution and/or storage of child pornography.** It is the hope of the International Centre for Missing & Exploited Children that this paper will help companies engage with partners in the digital world in a manner that allows for the protection of children and their company's reputation.

For more information write to information@icmec.org.

International Centre
FOR MISSING & EXPLOITED CHILDREN

1700 Diagonal Road, Suite 625 • Alexandria, Virginia 22314-2844 • USA
Tel +1 703 837 6313 • Fax +1 703 549 4504 • www.icmec.org