The ASACP Hotline Report

Online Child Pornography: Data & Analysis

CONTENTS

INTRODUCTION

Since 1996, the Association of Sites Advocating Child Protection (ASACP) has operated a child pornography (CP) reporting hotline. This document represents ASACP's analysis of data compiled from more than 400,000 reports of suspected child pornography received by that hotline during the five year period between January 1, 2005 and December 31, 2009.

ASACP is releasing this report to help further the goal of eliminating CP online. Stopping the flow of money to "commercial" child pornographers is a crucial part of this fight, and requires an understanding of strategies employed by these criminals, such as abusing legitimate online hosting and billing services in order to disseminate and profit from illegal images of child sexual abuse. Data collected by the ASACP Hotline therefore includes the geographic locations of servers hosting or processing payments for CP.

This report also addresses the issue of "non-commercial" CP – child pornography produced and/or distributed for reasons other than financial gain. Finally, ASACP's recommendations for meeting the rapidly and constantly evolving challenges of fighting CP and improving online child protection are determined by the analysis of current trends and possible implications for the future.

EXECUTIVE SUMMARY

Effectively combating child pornography (CP) requires a practical understanding of what CP really is, and how it is disseminated. Commercial Child Pornography (CCP) is distributed for profit, while Non-Commercial Child Pornography (NCCP) is offered free or exchanged in trade among pedophiles (an adult who is sexually attracted to children). Different strategies are called for in combating each. In addition to CCP websites that charge fees to members, NCCP circulates through various channels, including newsgroups, file sharing networks, message forums and other online communities. Some teenagers are also creating and sharing sexually explicit images and videos via the Internet. This is known as "sexting," and the resulting material fits the legal definition of child pornography, although these teens should not be treated as criminals.

CCP websites offer tens of thousands of images and thousands of videos. CCP operators gather images from a variety of locations using a variety of methods. Most children exploited in CP are pre-adolescent. Some victims appear to have been subjected to physical as well as sexual violence.

These statistics eliminate any confusion about the nature and intent of CP, the consumers of which are pedophiles seeking images of the sexual abuse of very young children. As a recent DOJ report noted: "Child pornography is unrelated to adult pornography; it clearly involves the criminal depiction and memorializing of the sexual assault of children and the criminal sharing, collecting, and marketing of the images." (United States Department of Justice, 2010. The National Strategy for Child Exploitation Prevention and Interdiction: A Report to Congress, p. 8.) Indeed, the adult entertainment industry's strong and consistent support for ASACP demonstrates an industry-wide commitment to protecting children and fighting CP.

CCP websites employ sophisticated and fraudulent traffic generation schemes, send out "spam" emails and instant messages (IMs), and utilize "bot" networks to remotely control compromised ("zombie") computer systems without the owners' knowledge.

ASACP operates an online CP reporting hotline, investigates reports and follows up with appropriate action. As of 2010, the ASACP Hotline has processed more than 500,000 raw reports. The ASACP Hotline receives as many as 12,000 raw reports per month. With the help of proprietary analytical software, these reports are categorized, with confirmed cases of child pornography generating "Red Flag" notifications. These are forwarded to the appropriate government agencies and associations, and they identify the hosting, billing, IP address, ownership, and linkage of the suspected CP sites. ASACP also notifies internet service providers (ISPs) and online payment processors when their web hosting and billing services are abused by CP operators.

Between 2005 and 2009, the ASACP hotline received 407,897 raw reports of suspected child pornography. The data collected reveals a steep drop in Red Flag reports since 2006. However, non-website reports of suspected child pornography grew rapidly between 2005 and 2008, before dropping again between 2008 and 2009. The data also identifies 161 countries (and all 50 United States) within the borders of which servers hosted or processed payments for commercial child pornography, or where CCP domains were registered.

During the five year sample period, the United States hosted the largest share of CCP websites, with 39.1% of global volume. By 2009, the United States' percentage had actually increased to 49.4%. This is unsurprising, since the largest concentration of hosting and billing services reside on servers in the U.S. However, CP content on U.S. servers rarely avoids detection and removal for very long. Furthermore, while the U.S. percentage share has grown, there has been a dramatic overall decline in the actual amount of CP images hosted within the borders of the United States, as web hosting companies have ramped up efforts to prevent, identify and remove illegal content. It is important to remember that servers hosting or processing billing for illegal material may be (and frequently are) located in an entirely different part of the world from where the actual CCP operators reside.

The United States was also the top country hosting billing for CCP websites between 2005 and 2009, with 12.5% of the total. By 2009, however, Spain had displaced the U.S., hosting 25.5% of CCP billing. However, the billing process exposes these criminal enterprises to the scrutiny of banks, credit card associations, internet payment services providers (IPSPs), and financial and regulatory agencies. To circumvent such scrutiny, CCP operators make fraudulent use of legitimate websites and the services of online billing companies, resorting to a variety of payment schemes to process their transactions.

The overall reduction in reports of CCP websites since 2005 may reflect billing companies' heightened vigilance, increased oversight by governmental and financial institutions, and the efforts of groups like the Financial Coalition Against Child Pornography, in which ASACP participates. Crucial progress has been made in blocking CCP operators from processing payments online, but continued vigilance is still required.

The teen "sexting" trend requires attention as well. However, felony prosecution of minors under child pornography statutes aimed at pedophiles, often resulting in teens being labeled for life as registered sex offenders, is misdirected. Likewise, attempts to fight child pornography by targeting the professional adult entertainment industry are unproductive, as CP is not related to adult entertainment.

As reports of CP websites have decreased, reports of non-website NCCP (newsgroups, file sharing networks, message forums and other online communities) have increased. Keeping pace with this change will require continuous reevaluation of strategies and priorities on the part of all organizations, government entities and other groups dedicated to stopping CP.

Localized efforts in many countries have focused on educating and empowering children and parents to prevent child sexual abuse before it occurs. However, not all countries have the infrastructure for such efforts. Therefore, some of the children most at risk require international assistance, which in turn requires increased international cooperation.

ONLINE CHILD PORNOGRAPHY

Under U.S. federal law, "child pornography" means depictions of minors engaged in sexually explicit conduct. That can include real or simulated sexual activity, as well as what is called "lascivious display of the genitals or pubic area."

This definition is useful from a legal perspective, but effectively combating CP also requires a practical understanding of what CP really is, and how it is disseminated.

COMMERCIAL VS. NON-COMMERCIAL

First, it is important to distinguish between Commercial Child Pornography (CCP), which is distributed for profit, and Non-Commercial Child Pornography (NCCP), which is offered free or exchanged in trade by and among pedophiles. The distinction is vital because different strategies are called for in combating each.

Websites are a common CCP venue because a fee can be charged to grant access to members. NCCP circulates through various channels, including Usenet newsgroup postings, peer-to-peer (P2P) file sharing networks, social media, message forums and other online communities, and directly between mobile devices. This complicates the mission of ASACP and other watchdogs, as already scarce resources are spread thinner and thinner in an effort to monitor and combat ever-evolving CP distribution mechanisms which now include mobile and social media spaces.

PREVALENCE & PRODUCTION

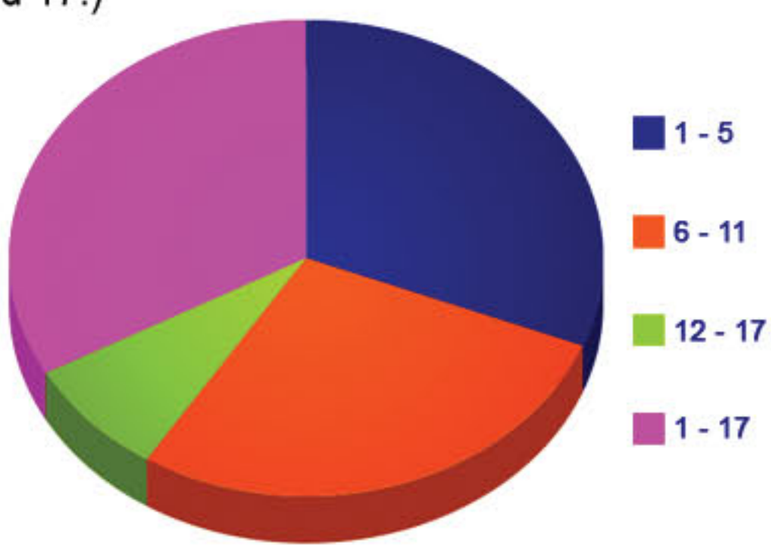
Second, while the subject is unpleasant and difficult, it is nonetheless useful and necessary to understand the range, type and volume of material circulating online that falls under the legal definition of CP.

Early CCP websites offered a limited number of images, mainly harvested from Usenet and BBS (Bulletin Board Systems), computer networks predating the World Wide Web. These images were often many years old and heavily re-circulated. However, ASACP hotline data points to a dramatic increase in the pool of available CP content in recent years. Today, CCP websites offer tens of thousands of images and thousands of videos in “premium” members-only sections.

To feed the demand for more and newer material, CCP operators are obtaining more content and updating “members” areas more frequently. The material is sometimes purchased from brokers, but operators gather images from a variety of locations using a variety of methods. Some CCP operators simply create the images themselves. Others harvest images from P2P networks, file hosting and sharing sites, BitTorrent (a popular file sharing application useful for transmitting large media files), other CCP websites, and vetted chat boards where members create CP by abusing children to whom they have access, in order to trade and gain access to new images.

THE VICTIMS

Most children victimized and exploited in CP are pre-adolescent. Of the CP images analyzed by the ASACP hotline 59% are children 11 and under: 31% featured children between 1 and 5 years of age. 28% featured children between 6 and 11. Children between 12 and 17 years of age accounted for only 8%. (The remaining 33% were mixed images depicting children of various ages between 1 and 17.)



(Figure 1: Ages of Children Depicted in CP)

Hotline investigators have also documented a qualitative shift, with images becoming more brutal and extreme. In these images, child victims often appear to have been subjected to physical as well as sexual violence.

ADULT ENTERTAINMENT VS. CHILD PORNOGRAPHY

These devastating statistics, outlining the very young ages of victims of online child sexual exploitation should eliminate any confusion about the nature and intent of CP. Consumers of CP are not in the market for "risqué" images of young-looking 18-year-olds. They are pedophiles seeking images of the sexual abuse of very young children. Likewise, CP operators are not webmasters of adult entertainment sites inexplicably risking long-term imprisonment by attempting to skirt age restrictions. As detailed above, CP operators are criminals trafficking in the most heinous material imaginable.

A recent DOJ report noted: "Child pornography is unrelated to adult pornography; it clearly involves the criminal depiction and memorializing of the sexual assault of children and the criminal sharing, collecting, and marketing of the images." (United States Department of Justice, 2010. The National Strategy for Child Exploitation Prevention and Interdiction: A Report to Congress, p. 8.) This finding is borne out by forensic analysis of CP images, as well as by ASACP Hotline data. Legal adult entertainment sites have been reported to the hotline, but only in error. By 2009, reporting of legal adult sites had dropped nearly to zero, signifying that such sites were no longer even being mistaken for CP.

Indeed, the adult entertainment industry's strong and consistent support for ASACP demonstrates an industry-wide commitment to protecting children and fighting CP. ASACP's Best Practices help adult sites avoid even the appearance of impropriety, and underage performers who have falsely represented themselves as adults using government issued documents have been quickly blacklisted and their videos immediately removed from circulation by the adult entertainment community. This kind of industry self-regulation represents both an ethical stance and a practical one, since adult entertainment businesses have no incentive to knowingly put themselves at risk when it comes to child pornography laws.

DISTRIBUTION

Since CCP websites are illegal and thus generally unable to promote themselves via traditional advertising and marketing techniques, they employ sophisticated traffic generation schemes. Complex systems of "feeder" sites – mislabeled websites and links in search engine listings – trick web surfers into clicking through to a CCP website's "doorway" page, which contains "teaser" content and links to billing pages. Thus, search engines and directories are likewise "tricked" into indexing CCP websites. Meanwhile, the feeder, doorway, billing and paid access content pages are often all hosted in different locations, utilizing different servers, under different legal and national jurisdictions. This "decentralization" makes it more difficult to track and detect CCP.

CCP operators also send out links via millions of "spam" emails and online message board postings, as well as unsolicited, fraudulent instant messages (IMs). They utilize "bot" networks – Internet connected computer systems infected by malicious code – which allow them to remotely control compromised computers ("zombies") without the owners' knowledge. Bots run hidden code in the background of normal operations, collecting email addresses stored on those compromised systems and turning them into email servers, which then send spam to large numbers of other systems, spreading the malicious code. Bot networks can also host child pornography content on an infected computer without the knowledge of the owner. This has obvious and frightening implications from a legal standpoint as well.

A NOTE ABOUT "SEXTING"

Though sometimes taboo, sexual expression among teenagers has always been a rite of passage. Among today's teenagers, electronic communication has become more common than face-to-face interaction. Unsurprisingly therefore, with the advent of smart phones equipped with Internet access and high-resolution digital cameras, some teenagers are now creating and sharing their own sexually explicit images and videos online. This is known as "sexting," and though it differs greatly from CCP and NCCP in terms of original intent (and ultimately, prevention strategy), the resulting material fits the current legal definition of child pornography. Such material can propagate beyond its intended audience, and join the pool of online CP redistributed and collected by CCP operators and pedophiles.

The teens involved can be prosecuted under child pornography statutes, although some states have passed, or are considering laws to more appropriately address this new phenomena. However, this is matter that needs to be and should be handled by parents rather than wasting already strained government resources.

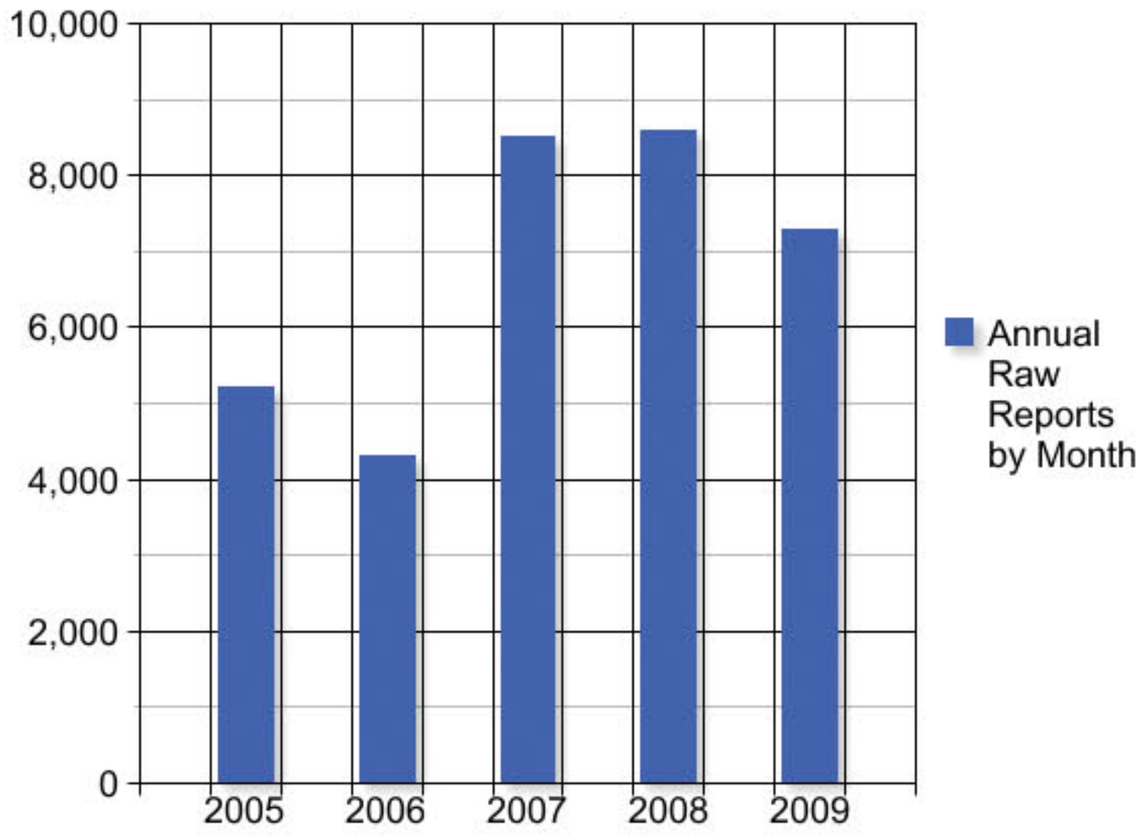
THE ASACP HOTLINE

ASACP operates an online CP reporting hotline where anyone can report suspected child pornography. Hotline staff members investigate all "raw" reports, and follow up with appropriate action (see below). As of 2010, the ASACP Hotline has processed more than 500,000 raw reports.

DATA TRIAGE AND ANALYSIS

The ASACP Hotline receives as many as 12,000 raw reports per month. In order to review, classify and investigate such a large volume of reports with minimal staffing resources, ASACP has developed custom proprietary analytical software that automatically recognizes and classifies spam, invalid web addresses ("bad" URLs) and duplicate reports. This enables hotline staff to review and investigate raw reports within 24 hours of receipt.

Figure 2 illustrates the average volume of monthly reports of suspected child pornography received by the ASACP Hotline, between 2005 and 2009.



(Figure 2: Average Monthly Report Volume, by Year)

CLASSIFICATION

After review and analysis, the ASACP Hotline staff separates these raw reports of suspected CP into 10 categories:

- **Red Flag (RF)**: Determined to be child pornography under U.S. Federal Law
- **Spam (SP)**: Not related to child pornography
- **Prior (PR)**: A duplicate report of a suspected child pornography website that was previously investigated by the ASACP Hotline
- **Non-Website (NW)**: Suspected CP disseminated via P2P (Peer to Peer), BitTorrent, newsgroups, web communities, chat/message boards, IM (Instant Messages) and IRC, chat rooms, etc.
- **Not CP (NCP)**: Reports that do not relate to child pornography under current U.S. Federal Law
- **Child Modeling (CM)**: Sites with clothed child models, also known as "non-nude"
- **Art**: Legitimate artistic renderings of children
- **Legal Adult (LA)**: Legal adult entertainment websites
- **Bad URL (BURL)**: Site was not active online when reviewed
- **Not Recorded (NR)**: An error occurred while the report was submitted or captured

CONFIRMED "RED FLAG" REPORTS

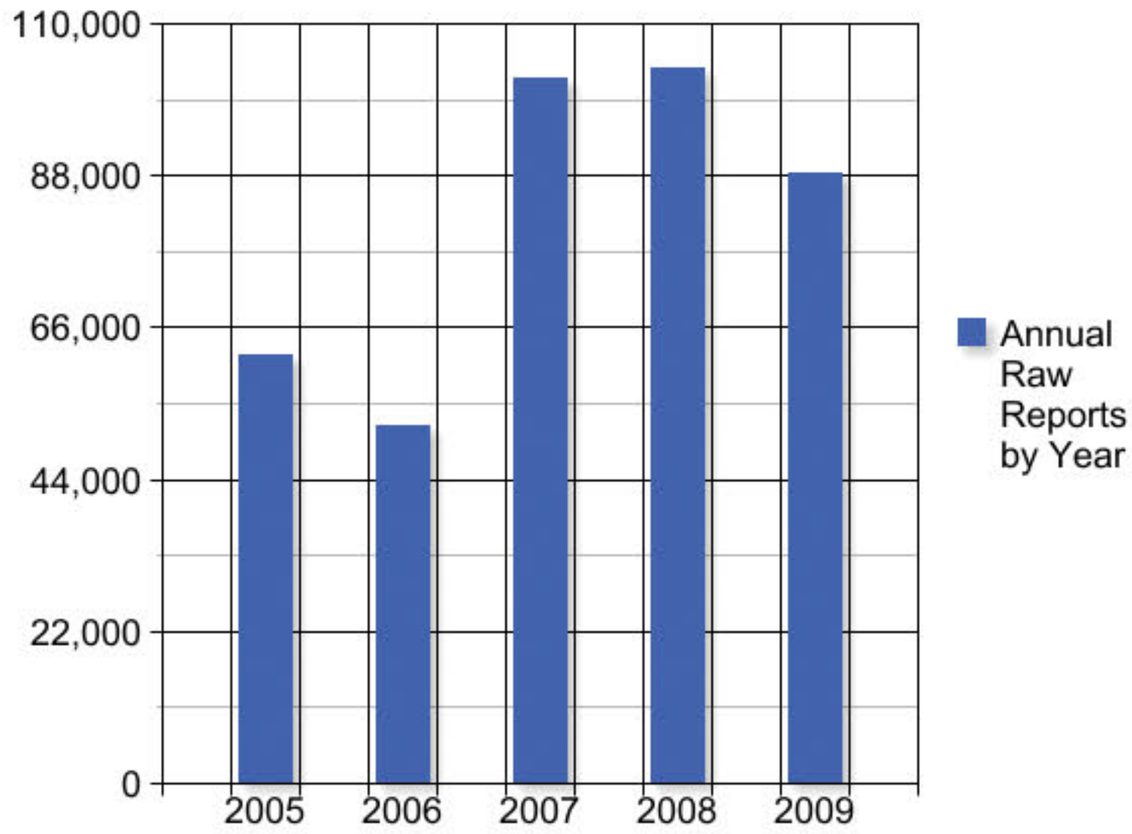
Once ASACP Hotline staff determines that a reported site may be child pornography, they identify the hosting, billing, IP address, ownership, and linkage of the suspected CP sites and forward "Red Flag" notifications to the appropriate government agencies and associations. These include the FBI, the Department of Homeland Security and the National Center for Missing & Exploited Children (NCMEC), as well as specific international hotlines depending upon the countries involved. ASACP also notifies internet service providers (ISPs) and online payment processors when their web hosting and billing
services are abused by CP operators. Finally, ASACP "scrubs" against its own membership database to verify that no ASACP member sites or their affiliate programs are being used to advertise or distribute CCP.

The data obtained from these reports provides law enforcement and other stakeholders with reliable information as to the sources of CP and the infrastructure that supports its commercial proliferation; it also provides insights into the evolving nature of online CP. ASACP's database has often been subpoenaed by law enforcement during the prosecution of child pornography cases.

HOTLINE DATA & ANALYSIS

RAW REPORTS

Between 2005 and 2009, the ASACP hotline collected 407,897 raw reports of suspected child pornography: 62,113 in 2005; 51,920 in 2006; 102,096 in 2007; 103,423 in 2008 and 88,345 in 2009 (fig. 3).



(Figure 3: Annual Raw CP Report Volume, by Year)

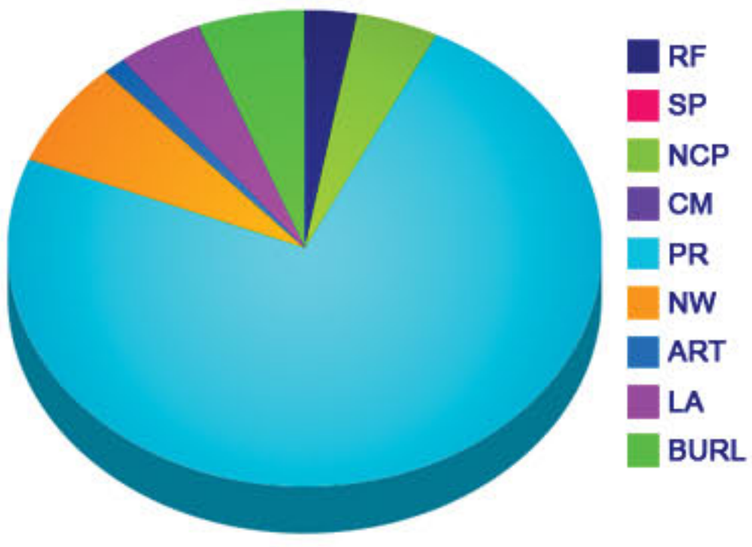
The following data summarize raw reports received by the ASACP Hotline, broken down by category, between 2005 and 2009:

RAW REPORT SUMMARIES: 2005-2009

2005

In 2005, the ASACP Hotline processed 1,742 Red Flag reports. The Hotline also received 45,412 duplicate reports that year, as well as 2,764 combined reports of non-CP, child modeling sites, and spam not related to child pornography. (Spam tracking began in 2007, and child modeling sites were designated a separate category in 2008, allowing for more detailed reporting in successive years.)

ASACP received 4,431 reports of CP on non-websites in 2005. Legal adult entertainment websites accounted for 2,866 reports (none of which contained CP) while 749 art websites presented legitimate artistic nude renderings of children; bad URLs totaled 3,601 of the reports (fig. 4).

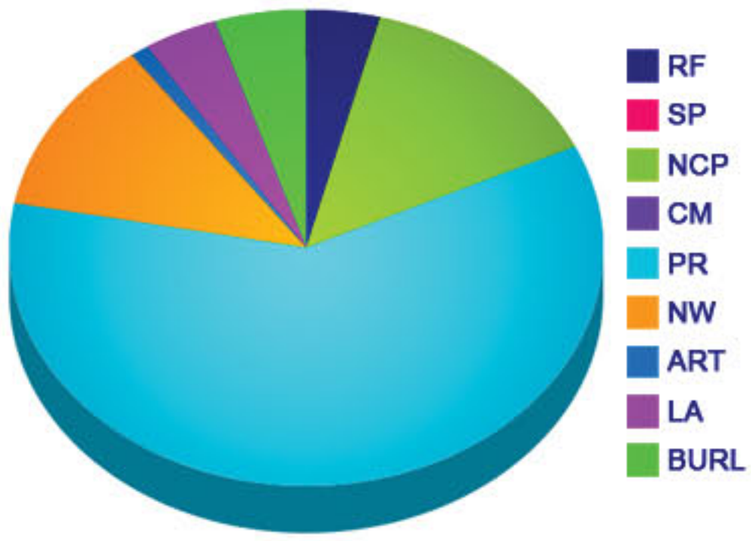


(Figure 4: Summary of Raw CP Report Data in 2005)

2006

In 2006, the ASACP Hotline processed 2,162 Red Flag reports. The Hotline also received 31,092 duplicate reports that year, as well as 7,427 combined reports of non-CP, child modeling sites, and spam not related to child pornography.

ASACP received 6,004 reports of CP on non-websites in 2006. Legal adult entertainment websites accounted for 2,094 reports (none of which contained CP) while 489 art websites offered artistic nude renderings of children; bad URLs totaled 2,547 reports (fig. 5).

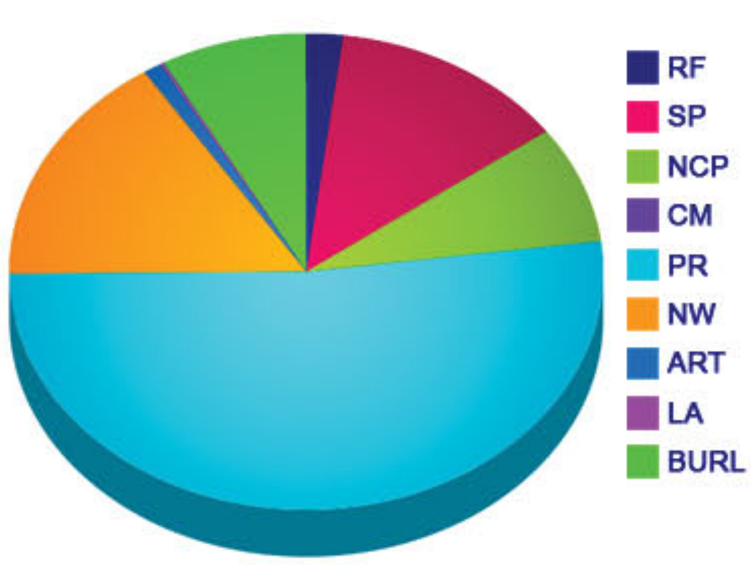


(Figure 5: Summary of Raw CP Report Types in 2006)

2007

In 2007, the ASACP Hotline processed 1,734 Red Flag reports. The Hotline also received 52,714 duplicate reports that year, as well as 8,466 combined reports of non-CP and child modeling sites. Spam with no relation to child pornography accounted for 12,684 reports in 2007 — the first year that the association tracked these submissions as a separate category.

ASACP received 16,184 reports of CP on non-websites in 2007. Legal adult entertainment websites accounted for 1,171 reports (none of which contained CP) while 224 art websites offered artistic nude renderings of children; bad URLs totaled 8,156 reports (fig. 6).

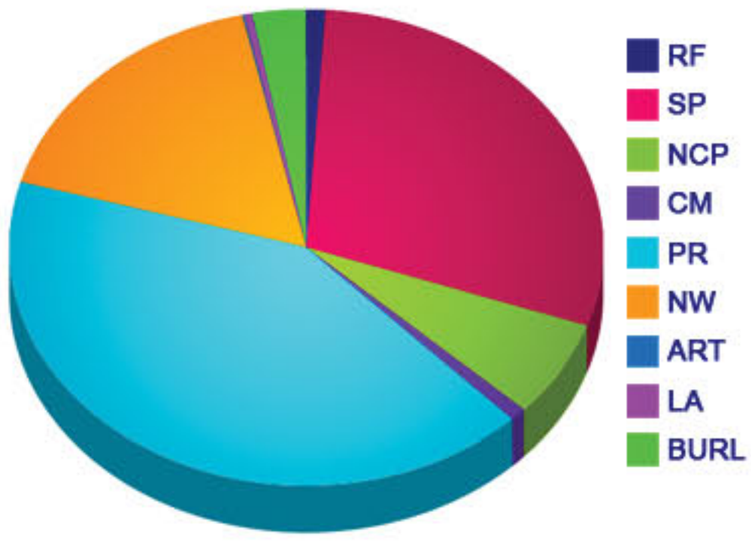


(Figure 6: Summary of Raw CP Report Types in 2007)

2008

In 2008, the ASACP Hotline processed 1,075 Red Flag reports. The Hotline also received 43,027 duplicate reports that year, as well as 6,821 reports of non-CP. Spam with no relation to child pornography accounted for 30,255 reports in 2008 — while 909 child modeling site reports marked the first year that the association tracked these submissions as a separate category.

ASACP received 17,651 reports of CP on non-websites in 2008. Legal adult entertainment websites accounted for 442 reports (none of which contained CP) while 106 art websites offered artistic nude renderings of children; bad URLs totaled 3,063 reports (fig. 7).

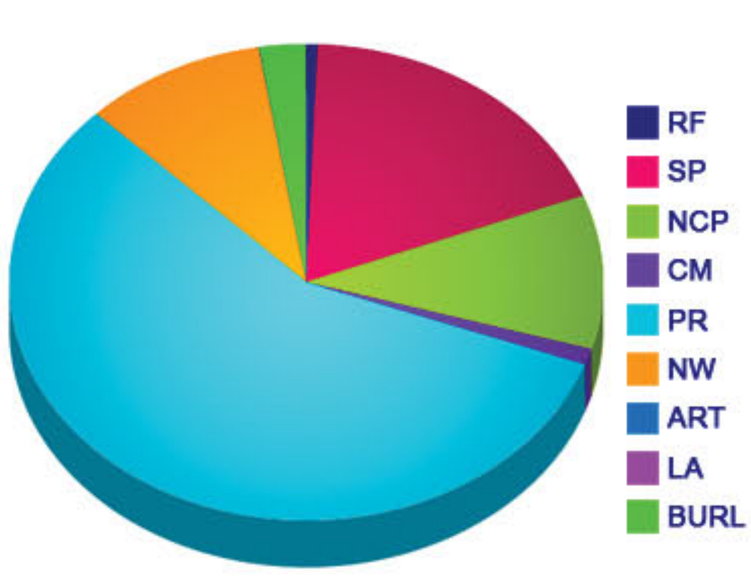


(Figure 7: Summary of Raw CP Report Types in 2008)

2009

In 2009, the ASACP Hotline processed 540 Red Flag reports. The Hotline also received 50,256 duplicate reports that year, as well as 9,256 reports of non-CP. Spam with no relation to child pornography accounted for 16,310 reports in 2009, with 941 child-modeling sites reported.

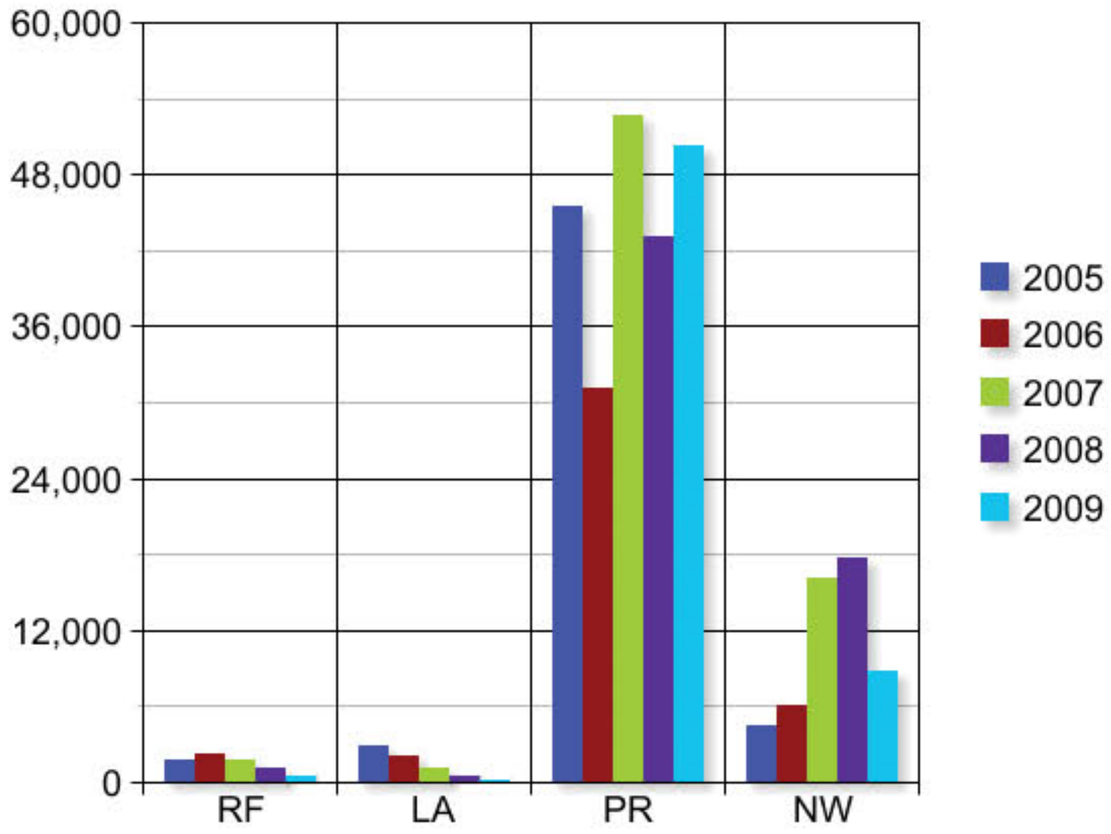
ASACP received 8,761 reports of CP on non-websites in 2009. Legal adult entertainment websites accounted for three reports (none of which contained CP) while 19 art websites offered artistic nude renderings of children bad URLs totaled 2,259 reports (fig. 8).



(Figure 8: Summary of Raw CP Report Types in 2009)

STATISTICAL TRENDS REVEALED BY HOTLINE DATA

- The number of unique annual Red Flag (RF) reports has dropped by 75% since 2006, when it peaked at 2,162
- The number of legal adult (LA) websites submitted to the hotline dropped from 2,866 in 2005 to only three in 2009
- Prior reports (PR) have remained relatively constant and account for the majority of raw reports, posting a five year average of 57%. The large number of duplicate reports is to be expected due to the methods used to advertise CCP websites (see DISTRIBUTION, above).
- Non-website (NW) reports of suspected child pornography grew 75% between 2005 and 2008. then dropped by 50% between 2008 and 2009

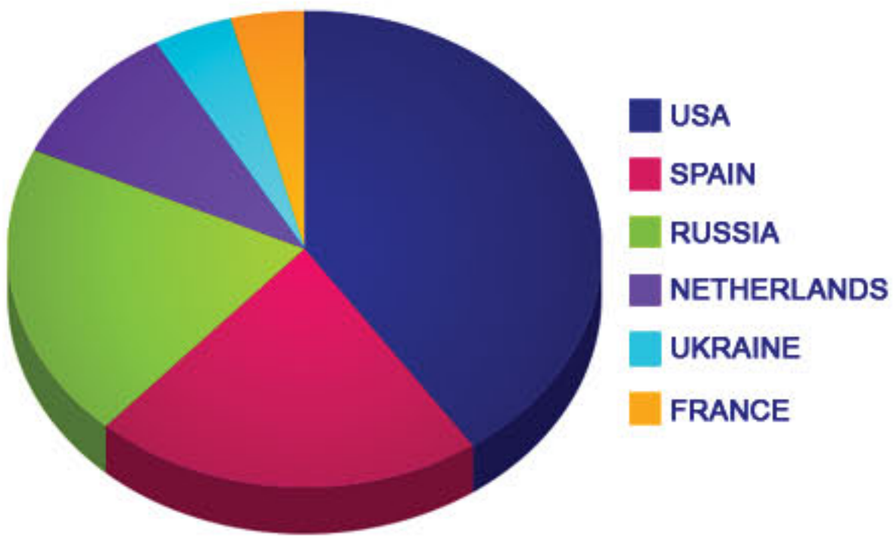


(Figure 9: Summary of Raw CP Report Types 2005 - 2009)

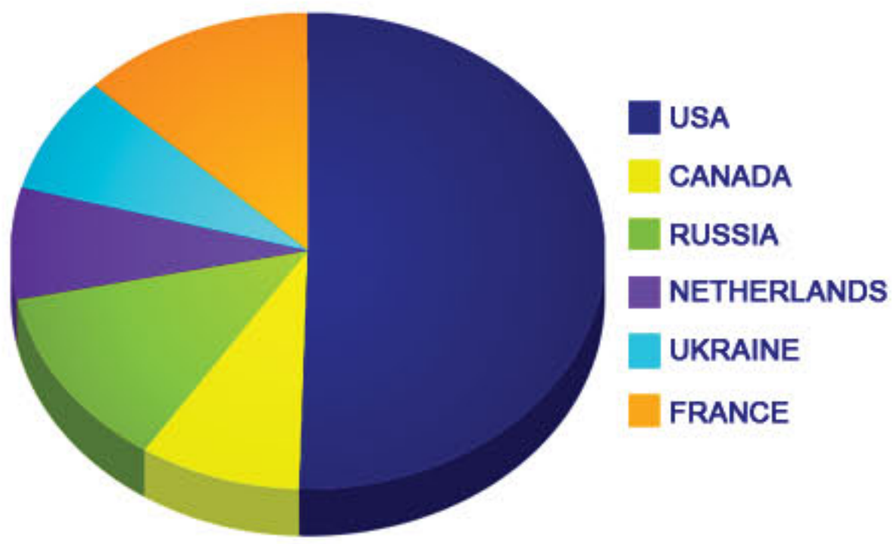
THE GLOBAL PERSPECTIVE

The illegal distribution of CP reaches virtually every wired corner of the globe. ASACP Hotline data collected between January 1, 2005 and December 31, 2009 identified 161 countries (and all 50 United States) within the borders of which servers hosted or processed payments for commercial child pornography, or where CCP domains were registered.

During that period, the United States hosted the largest share of CCP websites, with 39.1% of global volume. Other heavily impacted countries included Spain with 20.5%, Russia with 19.5%, the Netherlands with 9.5%, the Ukraine at 4.2%, and France at 3.9% (fig. 10). By 2009, however, the United States' percentage had actually increased to 49.4%. France's share rose as well, hosting 12.5% of CCP websites in 2009, followed by Russia's 12.2%, Canada's 8.6%, Ukraine with 7.8% and the Netherlands at 7.4% (fig. 11).



(Figure 10: Summary of Countries Hosting CP, 2005-2009)



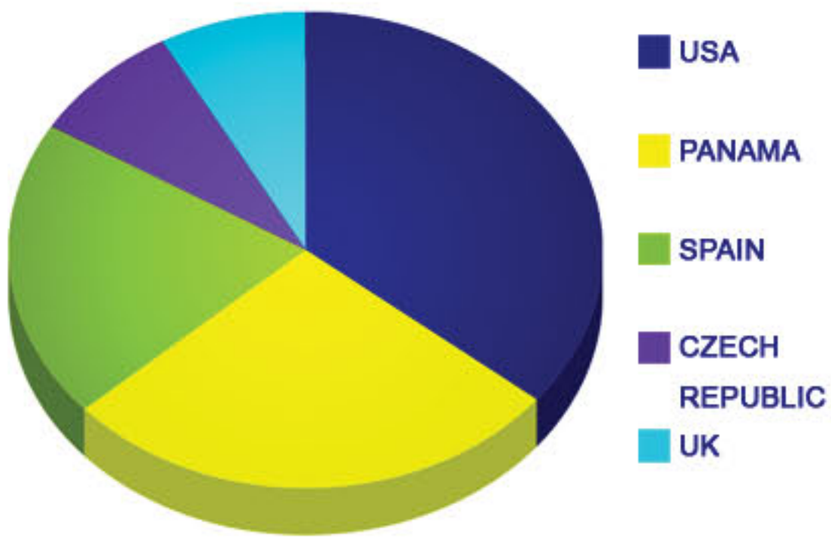
(Figure 11: Summary of Countries Hosting CP, 2009)

The United States' primacy here is unsurprising, since the largest concentration of hosting and billing services reside on servers in the U.S. However, CP content on U.S. servers rarely avoids detection and removal for very long. The vast majority of CCP websites hosted on U.S.-based servers remain online for only a few days, a reduction from an average of two to three weeks in 2005. By contrast, in some other areas of the world laws against child pornography are either non-existent, inadequate, or poorly enforced.

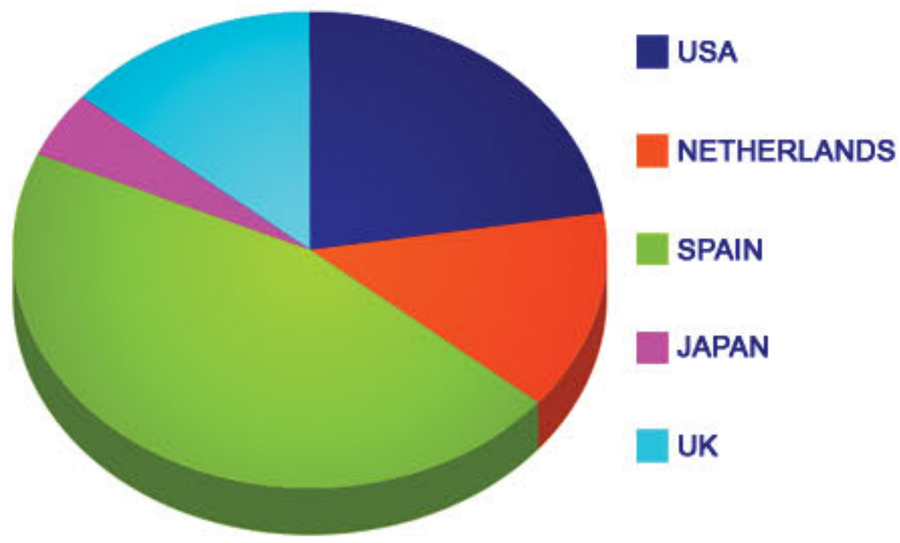
Furthermore, while the U.S. percentage share has grown, there has been a dramatic overall decline in the actual amount of CP images hosted within the borders of the United States, as web hosting companies have ramped up efforts to prevent, identify and remove illegal content from their servers via technological means, user-generated reports and increased staffing of abuse reporting departments. This increased scrutiny of account holders by web hosting services seems to be proving effective, but these companies need to remain vigilant and make sure their abuse reporting systems are easily accessible and user friendly.

It is also important to remember that servers hosting or processing billing for illegal material may be (and frequently are) located in an entirely different part of the world from where the actual CCP operators reside. However, the physical location of the servers involved does determine governmental jurisdiction and potential legal or regulatory interventions.

The United States was also the top country hosting billing for CCP websites between 2005 and 2009, with 12.5% of the total. Other heavily impacted countries included Panama with 9.6%, Spain at 7.1%, the Czech Republic with 2.9% and the U.K. at 2.8 % (fig. 14). By 2009, however, Spain had displaced the U.S., hosting 25.5% of CCP billing. The United States dropped to second place at 12.6%, followed by the U.K. with 7.8 percent, the Netherlands at 7.6% and Japan with 2.5% (fig. 12 & fig. 13).



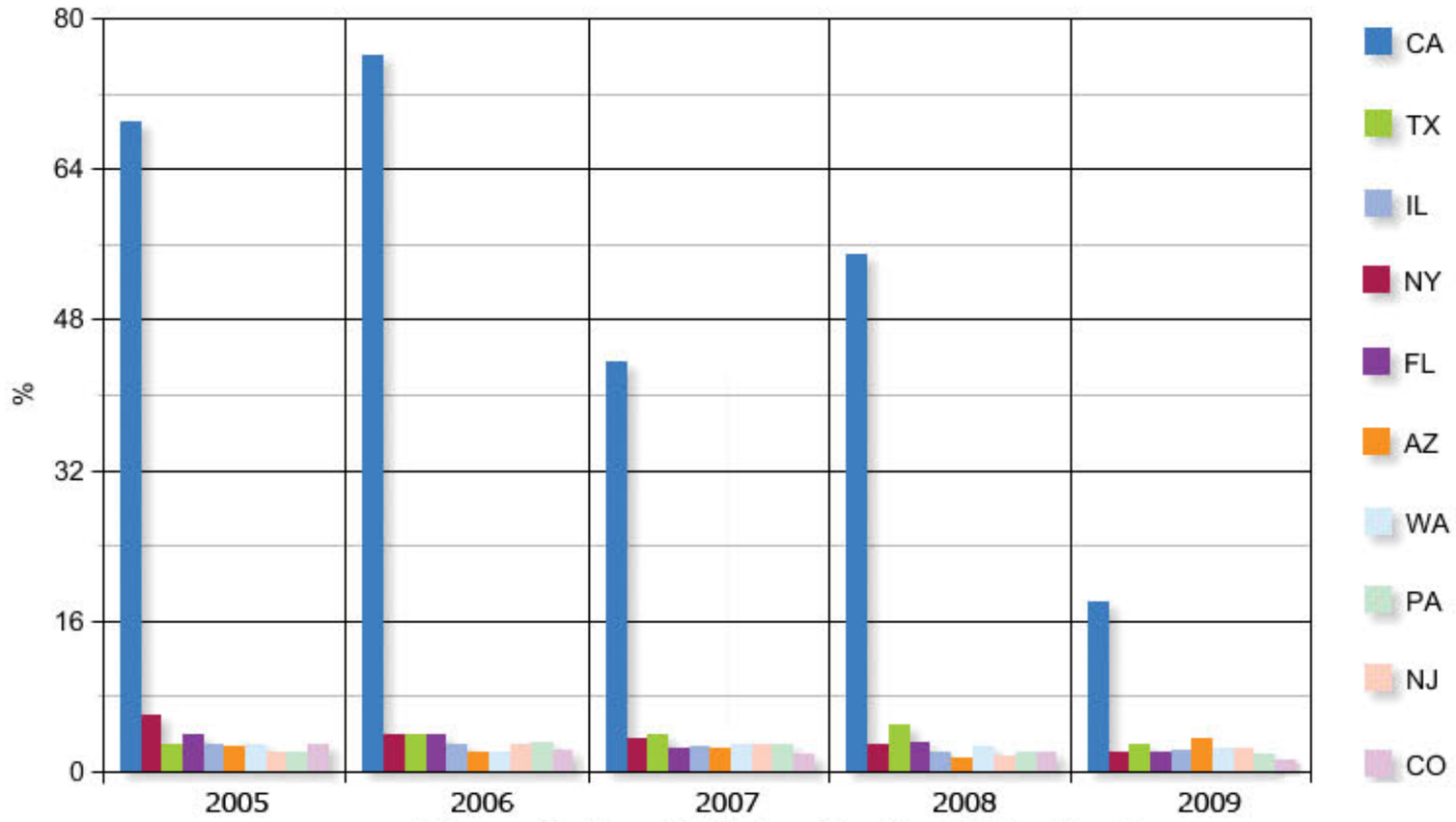
(Figure 12: Top Countries Providing CCP Billing, 2005-2009)



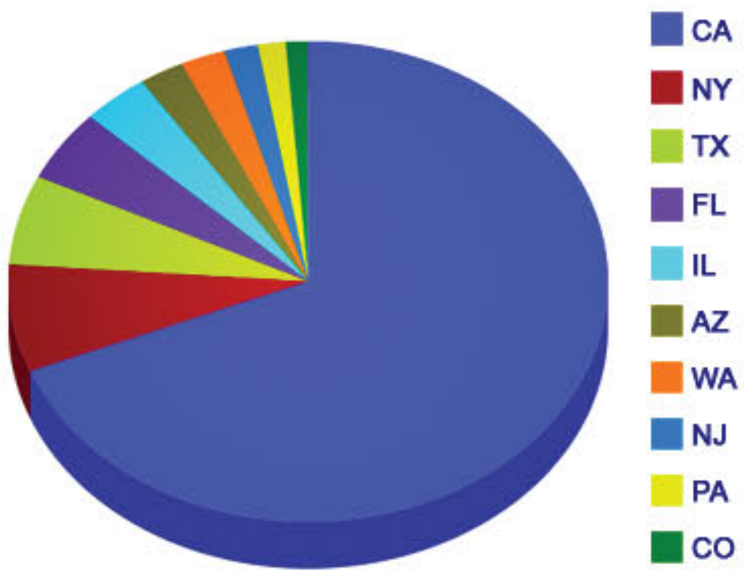
(Figure 13: Top Countries Providing CCP Billing, 2009)

CP HOSTING WITHIN THE UNITED STATES

Between 2005 through 2009, child pornography was hosted on servers located in all 50 United States. The following charts (fig. 14 & fig. 15) show the most impacted states, first by year and then averaged across the reported five-year span:



(Figure 14: Top 10 States Hosting CP by Year)



(Figure 15: Top 10 States Hosting CP – Five Year Average)

This data clearly reflects the high concentration of high-quality free hosting and user-generated content hosting services located in California, home to Silicon Valley and much of the computer industry. In addition, while high-quality free hosting services are available in a variety of locations, CCP operators seem to prefer to "hide in the crowd." Thus, the majority of CP hosting is on large-scale free hosts who rely heavily upon users reporting abuse, and for whom monitoring and detection are therefore a greater burden. Smaller hosting companies (for instance, those that provide services to the online adult entertainment industry) are less frequently abused by these criminals.

HOW LEGITIMATE COMPANIES ENABLE CCP BILLING

One major vulnerability of CCP operations is their need to process credit card or other online financial transactions, so customers can pay for their illegal images. This process exposes these criminal enterprises to the scrutiny of banks, credit card associations, internet payment services providers (IPSPs), and financial and regulatory agencies. To circumvent such scrutiny, CCP operators make fraudulent use of legitimate websites and the services of online billing companies, resorting to a variety of payment schemes to process their transactions. Some examples include:

Operating behind a "front"

This is fairly basic money laundering. Some CP websites do manage to obtain merchant accounts or IPSP processing, by setting up sham sites that sell non-existent merchandise. Nothing about these sites would appear questionable to reviewers. CCP operators then instruct CP-seekers to "purchase" some unrelated, legal item – say, a dozen roses – via a link to a site set up as a front. Instead of the roses, the buyer actually receives a child pornography DVD that is shipped to them, or access to an illegal CP site.

Using credit card loading mechanisms

In this scheme, CP websites direct potential subscribers to use a service like Western Union or Paypal, which applies payments or loads to a virtual credit card. Payments can then be applied to illegal purchases, with no apparent traces of the transactions. Facing ever-increasing scrutiny of e-commerce, some CP sites even require subscribers to submit their email addresses to receive billing links and information. By not displaying the billing company information on their websites, they make it harder for the transactions to be tracked and reported.

Hijacking affiliate programs

Affiliate marketing is a common online practice in which "affiliates" earn shared revenue (or commissions) by directing customers to an online business. CCP operators target affiliate programs (for example, software vendors) by instructing potential customers to buy legitimate products from an uninvolved company for which the CCP operator is a seemingly trustworthy affiliate. Once the fraudulent affiliate account has been credited, the CCP operator emails the CP-seeker the actual website, username and password for accessing the illegal material. The CCP operator receives the commission and gains direct access to the customer, while the legal business in the middle remains ignorant of the illegal transaction.

A bizarre twist

The ASACP Hotline has also uncovered credit card theft scams disguised as child pornography paysites. The operators of these sites solicit credit card numbers from pedophiles, but don't actually process these transactions but purchase other items. In other words, they use one crime to hide another crime. Obviously, the people who try to subscribe to these illegal sites are unlikely to call the police or complain to the Better Business Bureau. There is therefore no reliable data to compare how many are actually CCP sites versus how many are stealing credit cards and other personal information, in effect using one crime to perpetrate another, more lucrative one.

TRENDS & RECOMMENDATIONS

THE MONEY TRAIL

As noted above, there has been an overall reduction in reports of new and unique CCP websites since 2005. ASACP believes this reduction reflects substantial progress being made by governments, law enforcement agencies, child protection coalitions and related organizations in fighting the commercial exploitation of CP.

It is also likely that the decline specifically reflects billing companies' tightened content review policies, increased oversight by financial institutions, and the efforts of groups like the Financial Coalition Against Child Pornography, which brings together law enforcement, banks, credit card companies, online payment processors and internet service providers. As CCP operators' ability to find sustainable online billing options – especially domestically within the U.S. – is inhibited, so is the cash flow to this illegal industry. The Coalition works towards this goal by sharing information, analyzing how CP is bought and sold, finding effective intervention points, and determining ways to prevent those illegal transactions from taking place. ASACP participates in the Coalition, providing technical support and other resources.

Clearly, crucial progress has been made in blocking CCP operators from processing payments online. While this is a very positive sign, remaining CCP operators are likely to be well entrenched and thus more difficult to battle. Continued vigilance by all parties is called for to ensure that this hopeful trend continues. The ultimate goal is naturally to eliminate CCP by making it impossible for criminals to profit from the online sexual exploitation of minors.

ALL CHILDREN, EVERYWHERE

Localized efforts in many countries have focused on educating and empowering children and parents (as well as teachers and child care workers) to recognize potential threats and abusive situations, in order to prevent child sexual abuse before it occurs. This strategy aims to eliminate the preconditions for the creation of CP, and admirably so. However, not all countries have the social and practical infrastructure to initiate or implement such efforts. Particularly in very poor countries, laws against the sexual exploitation of children may be nearly non-existent or poorly-enforced. Pedophiles have been known to use online networks to discuss the best countries, cities, neighborhoods and even specific establishments where they can go to abuse children without legal consequences. This "sex tourism" phenomena must be addressed separately and in addition to the efforts to eradicate CP. Therefore, some of the children most at risk for exploitation may require international assistance, which in turn requires increased international cooperation to address the global issue of the sexual abuse and exploitation of children.

EFFECTIVE ALLOCATION OF RESOURCES

The teen "sexting" trend requires continued attention as well, both to prevent unwitting contributions to the pool of online CP material and to protect the teens themselves, who are often oblivious to the potential future consequences of their actions or even the possibility that such material might find its way into unintended hands. However, felony prosecution of minors under child pornography statutes aimed at pedophiles, often resulting in teens being labeled for life as registered sex offenders, is unwarranted. As with other risky and/or illegal behaviors like smoking, substance abuse and drunk driving, the key to protecting children (in this case, from themselves) is education and parental involvement. Otherwise society risks diverting already sparse enforcement resources, and diluting the effectiveness and relevance of sex offender registries.

Likewise, attempts to fight child pornography by targeting the professional adult entertainment industry are, at best, unproductive distractions; at worst a blatant waste of taxpayers' money. Endless legal wrangling has ensued from periodic attempts to expand 18 U.S.C. § 2257 (the federal law which mandates detailed record-keeping by producers of adult entertainment to ensure that models and performers are of legal age) – attempts predicated upon a false premise: namely, that the adult entertainment industry is eager to exploit minors. As ASACP Hotline data demonstrates, and as the previously cited Justice Department document notes, CP and adult entertainment are unrelated. The pedophiles and criminals

responsible for CP do not maintain records or care about regulatory laws, and are unhindered by such legal restraints. "Morality" campaigns that conflate adult entertainment and child pornography are not based on data, but on a censorship-driven agenda that sidelines the practical realities of fighting CP.

THE NEXT PHASE

As reports of CP websites have decreased, reports of non-website CP (disseminated via P2P and other methods) have increased. Non-website CP is also largely non-commercial CP, which means that there is no revenue stream to interrupt. Thus, one of the most effective anti-CCP strategies is useless against NCCP. For a combination of technical and legal reasons, most non-website reports are beyond the ASACP Hotline's legal capacity even to investigate.

This shift represents a sea change in the fight against child pornography. Keeping pace with these developments will require continuous reevaluation of strategies and priorities on the part of all organizations, government entities and other groups dedicated to stopping CP. Stakeholders must look beyond past roles and assumptions, proprietary attitudes and institutionalized methods.

To stop child pornographers, it is important to understand who they are and how they work. It is also essential to recognize who they are not, and apply valuable time, energy and funds accordingly.

ABOUT ASACP

Founded in 1996, ASACP is a non-profit organization dedicated to eliminating child pornography from the Internet. ASACP battles child pornography through its CP Reporting Hotline, and by leveraging the adult entertainment industry's financial backing and technical expertise to help eliminate the commercial trade in imagery depicting the sexual abuse of children. Through its Technology Taskforce of industry experts, ASACP provides support to a range of child protection groups in an effort to shut down CP distribution.

ASACP is member-supported, and offers a model of effective self-regulation for the online adult industry, including a Code of Ethics and Best Practices. Approved Members include adult entertainment and dating sites, content producers and distributors, support services providers (including web hosting, billing, traffic and software), merchant sites, affiliate programs, industry trade publications and traffic networks.

ASACP also works to help parents prevent children from viewing age-restricted material online, with its Restricted to Adults (RTA™) label. ASACP created the RTA label to better enable parental filtering. The RTA Label is free to use, voluntary, and universally available to any website that wishes to clearly and effectively label itself as being inappropriate for viewing by minors, simply by embedding simple code in the page header meta tags. This enables filtering via web browsers, ISPs, firewall/proxy servers, plugins, toolbars, commercial filtering software and even operating systems.

The RTA label may be applied to a single web page, an entire web site, or even a whole web server. First adopted by ASACP Members and Sponsors, RTA has since spread to those companies' affiliates and to innumerable other sites. As a result, some three million adult websites are already labeled with RTA, and the RTA tag is recognized by various filtering products and services. RTA also works with mobile devices, and an RTA app is forthcoming.

A recipient of the prestigious Associations Make A Better World award, ASACP has received recognition for its child protection efforts — including a Congressional Commendation from the U.S. House of Representatives — plus official certificates of recognition from the California State Senate and the California State Assembly. ASACP has also received various honors from the cities of Los Angeles, San Diego, San Francisco, Redondo Beach and West Hollywood.