Available online at www.sciencedirect.com

ScienceDirect

Aggression and Violent Behavior 12 (2007) 45 – 63

AGGRESSION AND VIOLENT BEHAVIOR

Cyber child pornography: A review paper of the social and legal issues and remedies—and a proposed technological solution

Bernadette H. Schell [a,*], Miguel Vargas Martin [a], Patrick C.K. Hung [a], Luis Rueda [b]

[a] University of Ontario Institute of Technology L, Canada
[b] University of Concepcion, Chile

Received 23 March 2006; accepted 28 March 2006
Available online 9 May 2006

Abstract

Cyber child pornography is an increasingly visible problem in society today. With the growth in home Personal Computer (PC) usage and more readily available access to the World Wide Web over the past decade, child pornographers have found a convenient venue for sharing horrific pictures of children being sexually abused. Also, police and lawyers around the globe have found that detecting and prosecuting cyber child pornographers have become onerous chores, often with a high failure rate of placing perpetrators behind bars. The methods currently employed by law enforcement officers to combat cyber child pornography may be considered to be primitive and inefficient. In this paper, we review the major social, legal, and technological issues facing citizens, lawmakers, and the police regarding cyber child pornography. We also propose a new technological approach for combating online child pornography. In particular, we propose a source address reputation system based on Bloom filters and a novel classification system utilizing a stochastic weak estimator, coupled with a linear classifier. We believe that our proposed method for identifying offensive online material would be attractive to law enforcement globally, because it can be implemented with acceptable overheads.

Keywords: Pornography; Personal Computers (PCs); Cyber child pornography; Internet; Website

Contents

* Corresponding author. Tel.: +1 905 721 3160; fax: +1 905 721 3167.
E-mail address: Bernadette.schell@uoit.ca (B.H. Schell).

1359-1789/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.avb.2006.03.003

> *Any technology throughout history has been adapted to two things—first of all pornography and secondly, the paranormal. —James Alcock* (McIlroy, 2005)

Specialized police in the United States, Canada, and Europe have been very busy since the year 2000 catching cyber criminals on the Internet who are intent on creating and distributing cyber pornography for a sizable profit. At the other end of the profit motive lies one or thousands of young children who are sexually abused and photographed for others' pleasures—typically males.

With the growth of the Internet from the 1990's through the present and with the decrease in price of Personal Computers (PCs) in recent years, child pornography sold over the Internet has become an increasingly visible problem for society, regardless of geographical and legal jurisdictions—for the Internet has no real borders. Furthermore, methods currently employed to combat online child pornography are considered even by the experts themselves to be rather primitive and inefficient. Given that typically multiple jurisdictions come into play for caught and convicted cyber pornographers, complex legal and technical issues exacerbate the problem significantly.

This review paper discusses the critical social and legal controversies and remedies surrounding cyber pornography—particularly the issues relating to online child pornography (known as cyber child porn). At the paper's end, we also discuss a proposed technological means of identifying offensive online materials that could be potentially attractive to law enforcement and could be applied in a cost-effective manner.

1. Introduction

1.1. A cyber child pornography case in point

Without question, child pornography is a subject often avoided in both social and research circles because of the heinous abuses that targeted children face, often for years without being saved. One such case was described in a recent popular media piece, written by Julia Morgan and entitled, “ruinyrpjs?”

This real-life drama unfolded as follows. A Toronto, Ontario, police officer by the name of Paul Gillespie just received about 450 images posted on the Internet by an officer in the United Kingdom—images of a little girl being beaten and raped. In several of the images, there was a hunting knife that was pointed at her, and on her little body were disgusting slogans like, “Kill me, I'm a slut.” Perhaps one of the most disturbing images was that of the little girl of about age five or six stuck naked inside a dog cage—with a terrified look in her big brown eyes. She was crying, and the corners of her mouth were turned downward. Using photo-editing software, Paul Gillespie was able to enlarge the contents of the images to determine the particulars surrounding the little girl's amusement park wristband and Girl Scout uniform number. The policeman then went to work using good old-fashioned police work. (Morgan, 2006).

The photo-enhanced leads eventually suggested that the little girl was a student in North Carolina. In just 36 h, the little girl was identified. When the Federal Bureau of Investigation (FBI) agents found her outside of an upscale house in a quiet suburban neighborhood, she appeared to be having fun riding on her bicycle. Inside the home was a male relative who put her through the abuse. During the arrest, FBI agents got five computers with 15 years worth of child porn, as well as cameras, weapons, a pair of dog cages, a Girl Scout uniform, to name just a few pieces of evidence. The man accused of the crime, a software developer, was apparently a well-respected citizen. But he was anything but. The relative belonged to a group of online child pornographers who created and watched "hurtcore"—explicit, hurtful images of children – younger than 13 and often just a few months in age – who were brutally sexually abused and in obvious pain. The captured relative of the little girl was not a very nice person. Just before his capture, he had brutally sexually assaulted a three-month-old male and had hired a fellow pedophile to murder his wife. The FBI agents prosecuting the case said they classified this man as one of the most evil pedophiles they had ever arrested. (Morgan, 2006)

1.2. What is known about child pornographers

There is no question that the Internet has caused the most explosive growth in child pornography than at any other time in history. One of the reasons for this explosion is that technology itself has greatly reduced the barrier to entry for the production and distribution of child porn. Cameras and powerful editing multimedia software are becoming more affordable and easier to use, simplifying the process of creating and distributing child porn. Child pornography, defined by federal law in the United States as "a visual depiction of a minor engaged in sexually explicit conduct," has been causing harm to children for centuries (Magid, 2002). But the Internet has given child porn new life because of the ease of transmission from one pedophile to many other pedophiles and from one country to many other countries.

The frightening reality is that at least 80% of those who purchase child pornography are active child molesters. Moreover, 36% of child pornographers who use the U.S. mail to exploit a child have been found to be actual child molesters. Child pornographers tend to range in age from 10 to 65 (Posey, 2005).

From a psychological profile perspective, psychologist Kimberly Young and Psychiatrist Alvin Cooper, two experts who have studied online sexual behavior, maintain that cyber sex (whether it involves minors or not) is a form of psychopathology and a symptom of neurotic, compulsive behavior. It is, without question, a type of addiction. Viewed as a type of socio- and psychopathology, cyber child pornography, in particular, is as an element of unhealthy power relations, whereby an adult abuses minors for his own pleasures. These acts of real-world abuse are often set into motion by adults having unhealthy sexual fantasies involving minors. For the most part, the cyber-supported sexual fantasy fulfillment with minors is found in ritualized practices and fixations, primarily of a sadistic sort (Uebel, 2002).

Pornography is progressive, besides being addictive, note the experts. As people become desensitized by the porn they see, they seek out more and more shocking material. It is, therefore, no surprise that child porn is becoming so vile and so prevalent on the Internet—with at least one-third of Internet traffic comprised of this type of shocking material. Not only are there pictures of penetrative sex by adults with two-month-old babies, but the Wonderland Club, which was discovered by the FBI and Scotland Yard in 2001, required prospective members to post 10,000 original images of child porn. That gives citizens around the world an idea of how many of these images there are in circulation (McAuliffe, 2001; McCafferty, 2004).

1.3. The depth of the problem

In 2005, TopTenReviews, Inc. estimated that child porn generates over $US 3 Billion annually (Ropelato, 2005), and over 100,000 Websites exist with the primary purpose of selling it to others, according to customs service estimates (BBC News, 2001a,b,c). Moreover, about 20% of the youths who frequent the Internet claim they have received sexual solicitations while online, and 89% of those who engage in online Chat Rooms say they have received such solicitations. What is quite alarming is that 29% of children aged 7 through 17 who frequently go online say they would freely give out their email addresses to others—making them ripe targets for online predators (Ropelato, 2005).

According to law enforcement agents, daily pedophiles exploit every aspect of the Internet, sharing children abuse tips and trading millions of "homemade" movies and photos of suffering children. Police estimate that anywhere from 25% to 50% of individuals viewing and trading cyber child porn have also committed acts of child sex abuse. Police further estimate that over 50,000 children worldwide are abused and used as child porn actors. Often, the children are bound, raped, and sodomized. Sadly, of this large number of children likely abused, apparently only a small fraction of them have been identified, and an even smaller fraction have been rescued by law enforcement officers. Adults engaged in cyber child porn are pleased to learn that many other like-minded adults exist, and they often utilize this reality to rationalize their own behaviors—which tend to escalate in aggressive acts – to hurtcore – over time. (Morgan, 2006)

1.4. How authorities learn about cyber child pornographers

Though an increasing number of law enforcement agents like Paul Gillespie are on the lookout for child pornography and its online perpetrators, many of the cases brought to their attention are reported by Internet users and Internet Service Providers (ISPs). Also, in 1998 in the United States, the CyberTipline (located at www.cybertipline.com) was created so that Internet users and ISPs could report online abuses, including cyber child porn and online enticement of minors to engage in sexual activities. Reports are then forwarded to federal law enforcement agencies, including the FBI, the U.S. Customs Service, and the U.S. Postal Inspection Service. Enticement of children for sexual favors is often started by an adult using an online Chat Room to arrange to meet a child—often done in a cunning way so that the child believes the perpetrator is trustworthy. As of March 2002, the CyberTipline received over 65,000 leads of online abuse, with the vast majority (over 55,000 leads) being cases of cyber child porn. This Website is maintained by the National Center for Missing and Exploited Children (NCMEC), with financial assistance from the U.S. Department of Justice and the U.S. Secret Service (Magid, 2002).

Also, the recipients of the 1998 U.S. Presidential Service Award the CyberAngels online group was founded in 1995 in the United States as the very first cyber-neighborhood watch group. Today, CyberAngels is considered to be the oldest group of volunteers concerned about the online safety of children and women. Their Website lists their mission as trying to function as a "virtual 411" safety destination. While supporting the right of free speech, they want to address parents' concerns about the safety of their children when they go online. These cyber volunteers are on the lookout 24 h a day, seven days a week for online abusers and cyber criminals. They report suspicious activities to legal authorities, and they produce documents to help parents assist their children in developing safe online habits (CyberAngels, 2005).

In 1999, the CyberAngels organization helped locate child pornography sites, resulting in the first-ever set of arrests in Japan of Internet child pornographers (Karp, 2000).

In other jurisdictions worldwide, cyber child porn detection units can be found. For example, in Canada there are the Toronto Child Exploitation Unit and at the Ontario Provincial Police (OPP) unit known as Project P. There is also the www.Cybertip.ca Website, where online users can report cyber child porn, and the advocacy group known as Canadians Addressing Sexual Exploitation. In the United Kingdom, there is the Internet Watch Foundation, and in Europe there is the COPINE Project, designed to combat pedophile networks (CBC News, 2003a,b).

Often, law enforcement agents affiliated with these child exploitation units pose as minors in Internet Chat Rooms (ICR), attempting to snare child porn perpetrators through acts similar to those employed by them to seduce children to meet them in public places. Many times, law enforcement agents are successful.

One such case occurred in August, 2005, in the Greater Toronto Area (GTA). An Ajax church pastor in the GTA by the name of Kenneth Symes, aged 36, was charged with attempted to have sex with a child after a man met face-to-face with whom he thought would be a 12-year-old female he had communicated with online for four months. The get-together was to occur in a public place in northwest Toronto. He was shocked when the child turned out to be Detective Constable Scott Purches from the Child Exploitation Section of the Sex Crimes Unit. The detective said that while in the ICR, the chat became more sexually explicit to the point where the perpetrator said he was willing to drive across the city to meet the child in a public place. The talks began in a Yahoo Chat room called Teen Oh Canada Chat, a well used teen Website. The pastor used the name "Garyneartoronto" in nearly forty conversations. He was married and had one child (Lai, 2005).

Since about 2000, international coalitions of law enforcement agents have worked in a similar manner to crack down on international cyber child porn rings. A major case in point occurred on August 8, 2001, when U.S. legal authorities arrested over 100 people for subscribing to an Internet site blatantly selling child porn. Authorities then said that they had cracked the largest child porn ring ever discovered. The Internet Website had more than 250,000 subscribers and was run from Texas, through operations in Russia and Indonesia. The child porn was also distributed through regular post (BBC News, 2001b).

The main culprits behind the online cyber child porn ring were a married couple from Texas, Thomas Reedy (aged 37) and his wife Janice, who worked as the company bookkeeper. The pair ran a company called Landslide Promotions and earned as much as $US 1.4 million a month on the operation—an indicator of how profitable the Internet can be as a distribution vehicle for child pornographers (BBC News, 2001b).

For two years, the company brought in almost $10 million in revenues, and both adults running the company drove Mercedes sports cars. During the police raid on their home, police seized dozens of computers and several servers, which led authorities to a list of 300,000 customers in 37 U.S. states and 60 countries. Subscribers to the Website paid about $30 with each access to the child porn Websites. It is interesting to note that since the couple did not produce the material – they acted as the middlemen, providing a Website to advertise pornographic material that was published in Indonesia and Russia – they did not believe they were doing anything illegal. The downfall came in the Reedy case when in April, 1999, several people complained to authorities about coming across his Website and noticing child porn. Calling his email address Houdini, Reedy openly advertised what he was selling on his web page: "Click here for Child Porn." In August, 2001, Thomas Reedy was sentenced to 1335 years in federal prison on 89 counts, including conspiracy to distribute child pornography and possession of child pornography. His wife Janice, who was convicted on 87 counts, received a prison sentence of 14 years. On appeal, Thomas' sentence was reduced to 180 years in prison, because the judge agreed that the original penalty was too harsh (CBC News, 2003b).

1.5. Social and legal issues surrounding online pornography and child pornography

In both a social and a legal sense, it is important to differentiate between online child porn – which is illegal in the United States and elsewhere – and online adult pornography—which is not necessarily illegal, unless the contents exceed the community's standard.

1.6. Adult pornography and child pornography

In short, adult pornography is deemed by most jurisdictions in North America and in Europe to be sexually-explicit material engaged in by "consenting adults." This type of material, for example, is protected in the United States by the First Amendment. What this means in real terms is that though a number of Websites, online newsgroups, and unsolicited email messages may offer adult pornography that is offensive in nature to many online viewers, these online venues are typically not in breach of the law. Though children may be portrayed in rather offensive poses, the models used by these adult porn Websites are typically over age 18 (Magid, 2002).

According to recent 2005 statistics, there are about 4.2 million pornographic Websites—about 12% of the total Websites in existence. The size of the pornography industry is about $US 57 billion worldwide-bringing in more revenues than the ABC, CBS, and NBC television networks combined, and more than the football, basketball, and baseball sports franchises combined. In 2005, over 40 million adults (72% male, 28% female) said that they regularly visited adult pornography Websites, and 20% of the men surveyed said that they regularly view pornography online while at work (Ropelato, 2005).

While laws against child pornography in the United States and in other jurisdictions worldwide have been designed and passed to protect children from exploitation, the reality is that children themselves often choose to go to adult pornography sites while online. According to recent 2005 statistics, the average age of a child's first exposure to online pornography is 11, the largest consumers of online pornography are in the age group 12-through-17, and 90% of 8-through-16-year-olds have viewed pornography online-most, they admit, while doing their homework. What is alarming is that about 29% of the 7-through-17-year-olds said that they would give out their home addresses to others while online (Ropelato, 2005).

1.7. Commonalities between the internet and the 1980's dial-a-porn

It is important to note that while the Internet may be charged by parents and by lawmakers as being an overly accessible route to children to view pornographic materials, back in the 1980s, "dial-a-porn" telephone services had the same allegations. Briefly, these telephone services offered sexually-explicit messages, live or prerecorded, for a fee. As a result of its popularity, "dial-a-porn" telephone services angered many parents when there were dramatic increases in their telephone bills—often brought on by a keenness to listen to the explicit sexual messages by their own children and their friends. Too, parents were angered at their children's easy access to dial-a-porn content. As a result of public outcry, the U.S. Congress acted quickly to create a specific criminal offense to control dial-a-porn services. But after a decade of court hearings and complex interactions between the Federal Communications Commission (FCC), the courts, and Congress, the United States was finally able to achieve a comfortable resolution to the dial-a-porn issue (Mashima & Hirose, 1996).

For example, to respond to the negative allegations of the "dial-a-porn" telephone services by its citizens, in 1983, U.S. Congress amended the Telecommunications Act to stop the dissemination of obscene or indecent commercial television services in interstate or foreign communications to minors under age 18. The amended Act imposed stiff penalties of fine, imprisonment, or both for violations of the Act. Then, one year after the Act's passage, the FCC said that dial-a-porn services could only be conducted between the hours of 9 PM and 8 AM to prevent children from seeing the potentially harmful material, and that payment by credit card (presumably, an adult's) had to be received before a sexually-explicit message could be sent. However, a court case was immediately launched on the grounds that this ruling was infringing on adults' freedom of information rights, and the Federal Appeals Court for the Second Circuit invalidated this time-of-day restriction, finding that the FCC could have adopted some other alternative that did not severely restrict free speech. So, in 1985, the FCC proposed a new idea: dial-a-porn content providers could transmit sexually-explicit content only to callers using an access code or personal identification code (PIN)—available only to adults (Mashima & Hirose, 1996).

A Second Circuit court heard an appeal questioning the legality of the new regulation in areas served by New York Telephone, where implementing the access code restriction was not feasible because of a one-way, non-interactive system. As a result, the FCC again amended its approach, adding another defense: message scrambling plus credit card payment, with sales of decoders limited to adults by state law. Then in 1988 – an election year – Congress said that it would explicitly prohibit not only "obscene" content in dial-a-porn messages but "indecent" commercial telephone communications directed to anybody regardless of age, including adults—in essence, a total dial-a-porn ban. In 1989, another U.S. Supreme Court case ensued; it continued with its distinction between indecency and obscenity by upholding the ban on "obscene" interstate commercial telephone transmissions but rejected the ban on "indecent" telephone messages. In the end, Congress amended the Act not to prohibit but to regulate "indecent" telephone communications. In 1990, the FCC adopted final regulations to establish defenses to prosecution under the Act: credit card authorization, use of PIN codes, and scrambling of transmissions (Mashima & Hirose, 1996).

1.8. The legal objectives of online child pornography legislation

Turning now to online child pornography, it is clear that punishing perpetrators of the act involves a classic legal balancing act between safeguarding minors and preserving the information rights and freedoms of adults. In short, lawmakers in North America and in Europe have generally attempted to weigh the protection of children from sexual exploitation against the protection of free speech and free thought. In the United States, the latter are protected under the First Amendment, and in Canada, the latter are protected under the Charter of Rights and Freedoms.

The general problem, as exemplified in the U.S. dial-a-porn illustration, is that if lawmakers lean too far one way, the courts will strike down the law, affirming that it infringes on the rights of citizens. If the lawmakers lean too far the other way, legal authorities and the police will maintain that they are being hampered in their fight against cyber criminals by "toothless laws" when trying to catch and convict, say, cyber child pornographers.

Added to this debate is the reality that in the United States, in Canada, in South Africa, and elsewhere around the globe, often as a reaction to some heinous crime to innocent children, laws are hastily passed to stop and convict criminals, including cyber pornographers. Moreover, because technology is continuing evolving, so do the laws that pertain to technology, including the Internet.

1.9. A closer look at Canadian cyber child porn legislation

For example, Canada's Criminal Code outlines penalties for various crimes, including those of a cyber nature. In 1993, the Criminal Code was amended to create a new prohibition order-lasting up to a lifetime—to prevent convicted child sex offenders from visiting any place where children tend to be: day-care centers, school grounds, playgrounds, or public parks. The order also prohibited convicted child sex offenders from seeking or keeping paid or volunteer positions of trust or authority over children. Another provision was created to allow an adult to obtain a peace bond (i.e., a protective order lasting up to one year) if he or she feared that another adult would commit a sexual offence against a child. Also, in May 1997, Bill C-27 amended the Code to allow for the prosecution in Canada of Canadian citizens or permanent residents who sexually abused children while abroad. In September, 2000, Canadian federal, provincial, and territorial justice ministers proposed an amendment to the Criminal Code making it an offense to use the Net to lure children for criminal purposes. Then, less than two years later, the Canadian government enacted Bill C-15 A in July 23, 2002. It brought into force child exploitation laws dealing with two main issues: Child pornography on the Internet and using the Internet to lure children (Department of Justice Canada, 2002).

In short, today's amendments to the Criminal Code address the reality of new technologies. Lawmakers have added to the list of possible banned activities the use of the Internet to communicate with children for sexual purposes. These amendments also include crimes related to child porn and Internet-luring as offences for which an offender would be subject to either a prohibition order that could last up to one's lifetime or a one-year peace bond. The changes also mean that child pornography and luring offences are added as offences for bringing an application for an offender to be designated as a "long-term offender." An individual such designated can be made subject to community supervision lasting up to 10 years. The Criminal Code now defines "child porn" as "a photographic, film, video, or other visual representation, whether or not it was made by electronic or mechanical means…that shows a person who is or is depicted as being under the age of 18 years and is engaged in or is depicted as engaged in explicit sexual behavior…or the dominant characteristic of which is the depiction, for a sexual purpose, of a sexual organ or the anal region under the age of 18 years…or any written material or visual representation that advocates or counsels sexual activity with a person under the age of 18 years…"(Department of Justice Canada, 2002).

It is important to note that the child pornography law was rushed through Canadian Parliament in fewer than six weeks, and it became law on June, 23, 1993, after which Parliament adjourned for the summer. Even the Members of Parliament who helped frame it said it was a hastily-passed piece of legislation that was overly broad, with little thought given to the protection of the Charter of Rights and Freedoms. Before leaving for the summer, certain Members of Parliament said that if the Act did not pass the test, then it could be corrected later on.

1.10. Legal cases testing Canadian child porn legislation

The first case to test the 1993 child porn piece of legislation was a February, 2000, case in which a Toronto artist by the name of Eli Langer, age 27, was charged under the new law for his showing of paintings of individuals having sex. Some appeared to be young males under age 18. The judge hearing the case ruled that the works had "artistic merit, "and the charges were dropped. However, the Ontario government used a forfeiture application to seize the work as being "child porn," with the intent of destroying it. At the end of the deliberations, the paintings were returned to Langer (CBC News, 2006a,b).

Another highly contentious child porn case that made it to the Supreme Court of Canada in January, 2001, involved perpetrator John Robin Sharpe, aged 67, a retired city planner living in Vancouver, British Columbia, Canada, who was charged with possessing child porn in 1995. The man was found to have pictures of boys under age 14 engaging in sexual acts. He also had a collection of his own stories involving sexual acts of minors, entitled, "Kiddlie Kink Classics." Two lower British Columbia courts had acquitted Sharpe of the charges, citing the Charter of Rights and Freedoms. The Supreme Court upheld most of the law, but found that adults cannot be prosecuted for producing written or visual materials or works of their own imagination – no matter how sexually explicit – for their own use. The Supreme Court of Canada then sent the Sharpe case back to the BC Supreme Court for retrial in January, 2002. In March, 2002, the Court found the accused not guilty of possessing written child porn, but Sharpe was found guilty on two counts of possessing pornographic pictures of children. He was later sentenced to four months of house arrest. Two years later in March, 2004, Sharpe was found guilty of a separate charge of indecent assault. These charges were grounded in an incident that took place twenty years ago involving a 14-year-old hitchhiker. Sharpe was acquitted of the second charge of sexual assault (CBC News, 2006a,b).

It is interesting to note that in December, 2002, the Canadian federal government proposed new legislation removing the defense of artistic merit in cases of works of imagination involving sexual acts of minors, with the material being judged in the courts on whether it contributed to the "public good"—the standards of society. Arts groups said that it would place an unfair burden for artists working on "edgy areas," including controversial movies like "The Boys of St. Vincent," which dealt with the abuse of boys in a Canadian orphanage. The bill to amend the definition of child porn, therefore, died on the ledger when the 2004 election was called. Of interest, during that election, public outcry to toughen the Criminal Code was related to the criminal case of Michael Brier, a pedophile murderer of 10-year-old Holly Jones. The accused admitted that his fantasy about having sex with minors was increased by his engaging in Internet child porn (CBC News, 2006a,b).

1.11. Summary of the legislative issues

In summary, there is little question that how one defines pornography – adult porn or child porn – depends to a large degree on how one views it. Literally, the word pornography means "the graphic depiction of whores." Dines has said that from a historical function, any product produced for the primary purpose of facilitating male arousal and masturbation can be deemed pornographic (Morgan, 2003).

Throughout history, including the recent past, religious conservatives have defined pornography as being immoral, while anti-pornography feminists view pornography as liberating, particularly in terms of sexual freedom. This definitional conflict is, without question, at the heart of the problem of pornography. Is it protected speech – at least in some forms – or is it a violation of human equality rights—particularly if children are involved in sexual acts with adults? Lawmakers and legal authorities have generally taken the view that pornography can be seen as a record of harm in its production—specifically to children and women, and more recently, to non-dominant males (Adams, 2004).

Pornography is not simply words that may offend some in society but records of acts—causing harm and pain to unwilling victims. For example, in pornographic images, anal intercourse is usually depicted without any use of lubricant on the victims. Moreover, while pornography's clientele may have changed over the past 30 years of women's lib to include women, the primary target audience of pornography in 2006 is males. Some women's groups have argued that males showing females pornography as a sexual aid to better sex must, instead, be viewed as a form of "grooming" behavior. The latter is a term describing how a child sex abuser uses various techniques, including showing porn to children, to lower their defenses and to get them to accept the sexual acts as "normal" rather than "abnormal" or "abuse." In closing, many questions remain regarding the definition of and legal applications to pornography, in general, and child porn, in particular. Can sexuality and sexual practices, for example, be separated from the construction of gender or age? Moreover, when an act is sexual, is it harder to see the harm that it represents to targets other than the intended audience? These are key aspects of the debate that seems to be ongoing, regardless of the evolution of technology (Adams, 2004).

1.12. Laws passed in the United States and elsewhere for curbing online child pornography

How Canada has made recent amendments to its Criminal Code to curb online child pornography has just been discussed. Other jurisdictions over the past six years have taken similar steps. Key among these has been the United States and European nations.

In the United States, crimes committed over the Internet place in the general category of "cyber crimes," because they are committed in cyber space and involve breaches of privacy, security, and trust. Therefore, harm resulting from these acts over the Internet can be to either persons or to property. There are also technical non-offenses, for which in the North America context, no legislation declares the acts as unlawful – such as hacktivism – whereby an individual uses a computer or computer networks to advance one's political agenda (Brenner, 2001, June).

1.13. Criminal liability elements and harm to persons

For old-fashioned or Internet crimes to occur, Anglo-American law bases criminal liability on the coincidence of four elements (Brenner, 2001):

- A culpable mental state (the *mens rea*).
- A criminal action or a failure to act when one is under a duty to do so (the *actus reus*).
- The existence of certain necessary conditions or "attendant circumstances." With some crimes, it must be proven that certain events occurred, or certain facts are true, in order for a person to be found guilty of a crime.
- A prohibited result, or harm to property or to person.

Most U.S. states and the federal government outlaw the possession or distribution of pornography. The obscenity statutes make it an offense to knowingly display obscene materials. Cyber porn uses a computer to display and/or distribute obscene materials.

Thus, the four elements of criminal liability for cyber pornography, in general, can be described as follows: the *actus reus* is displaying obscene materials using a computer; the *mens rea* is doing so knowingly; the attendant circumstances are that the material is obscene; and the harm is the dissemination of obscenity over the Internet. Moreover, with child porn, U.S. statutes state that it is an offense to either knowingly possess material that visually or aurally depicts a child under age eighteen engaged in sexual activity, or to bring or cause such material to be brought into the state, or distribute such material in the state, or publish or otherwise issue such material with the purpose of distributing it in the state (Brenner, 2001).

Thus, the four elements of criminal liability for cyber child pornography, in particular, can be described as follows: the *actus reus* is possessing, importing, distributing, publishing, or otherwise issuing child pornography using a computer; the *mens rea* is knowingly possessing or purposefully importing, distributing, or issuing child pornography; the attendant circumstances are that the material is child porn; and the harms are that minors are used to create child porn, and that child porn is disseminated through the Internet to those finding it appealing and stimulating (Brenner, 2001).

1.14. Common types of cyber harm to property

Internet cyber crime resulting in property harm is generally accomplished with certain computer skill sets and includes common variations like the following (Schell & Martin, 2004):

- Flooding—a type of Internet vandalism resulting in Denial-of-service (DoS) to authorized, legitimate users of a Website or computer network.
- Virus and worm production and release—a type of Internet vandalism causing corruption, and possibly erasing, of data stored on the network.
- Spoofing—a type of appropriation of an online user's identity by others online, caused fraud or attempted fraud in some cases, as well as critical infrastructure breakdowns in other cases.
- Phreaking—a type of Internet fraud consisting of using technology to make free telephone calls.
- Infringing Intellectual Property Rights (IPR) and Copyright—a type of Internet theft involving the copying of someone's information or software without getting their consent.

1.15. Common types of cyber harm to persons

Internet cyber crime resulting in personal harm includes two major variations (Schell & Martin, 2004):

- Cyber stalking—using the Internet to try to control, harass, or terrorize another online user to the point that he or she fears harm to reputation or to person (including death), either to self or others close to him or her.
- Cyber pornography—using the Internet to possess, create, import, display, publish, or distribute pornography (especially child pornography) or other obscene materials.

Because of the relative anonymity offered by the Internet and the users' capacity to create and amend visuals using online graphics and software technology, cyber pornography – and cyber child porn, in particular – have soared over the past decade. Those opposing child porn and adult porn have consistently argued that they present as major moral and personal harm problems for modern-day society.

1.16. A closer look at U.S. cyber child porn legislation

As noted earlier, in the United States, child pornography is a category of speech not protected by the First Amendment. The federal legal definition of child pornography can be found at 18 U.S.C. § 2256. Some particulars around the definition have changed in recent years, with the latest change occurring on April 30, 2003, when President George W. Bush signed the PROTECT Act.

The latter not only implemented the Amber Alert communication system – which allows for nationwide alerts when children go missing or are kidnapped – but redefined child pornography to include not only images of real children engaging in sexually explicit conduct but also computer-generated depictions indistinguishable from real children engaging in such acts. *Indistinguishable* was further defined as that which an ordinary person viewing the image would conclude is a real child engaging in sexually explicit acts. However, cartoons, drawings, paintings, and sculptures depicting minors or adults engaging in sexually explicit acts, as well as depictions of actual adults that look like minors engaging in sexually explicit acts, are excluded from the definition of child pornography.

The PROTECT Act of 2000 was passed because of three major problems that still existed, despite legislation (U.S. Department of Justice, 2003). These were as follows:

- Law enforcement did not have the tools needed to locate missing children and to prosecute offenders.
- Existing federal laws did not ensure adequate, and at times, consistent punishment for those found guilty of such crimes.
- Past legal obstacles have made prosecuting child pornography cases very difficult—especially virtually-produced child pornography. For example, in the April 16, 2002 high court decision, virtual child pornography that appeared to involve – but did not actually include – identifiable juveniles was entitled to free speech protection. To avoid conviction, defendants frequently raised the theoretical possibility that rapidly-advancing computer imaging technology was involved in the production of the materials, not real children. (Frieden, 2002)

Prior to the enactment of the PROTECT Act, the definition of child pornography came from the 1996 Child Pornography Prevention Act (CPPA). Moreover, the Children's Online Privacy Protection Act (CIPA), effective April 21, 2000, applied to the online collection of personal information from children under age 13. The rules detailed what a Website operator must include in a privacy policy, when and how to seek verifiable consent from parents or guardians, and what the responsibilities an operator has to take to protect children's privacy and safety online. It is important to note that these Internet safety policies required the use of filters to protect against access to visual depictions considered as obscene or harmful to minors (Miltner, 2005).

A filter is a device or material for suppressing or minimizing waves or oscillations of certain frequencies. Therefore, filtering software should block access to Internet sites listed in an internal database of the product, block access to Internet sites listed in a database maintained external to the product itself, block access to Internet sites carrying certain ratings assigned to those sites by a third party or that are unrated under such a system, and block access based on the presence of certain words or phrases on those Websites. In short, software filters use an algorithm to test for appropriateness of Internet material—in this case, for minors.

Websites are first filtered based on IP addresses or domain names. Since this process is based on predefined lists of appropriate and inappropriate sites, relying totally on these lists is ineffective because Internet sites come and go so quickly. Moreover, though minors often frequent online Chat rooms, instant messaging, and newsgroups, these are not under the filtering system but are a real point of concern for society (Miltner, 2005).

1.17. A closer look at child pornography in other jurisdictions

In 2002, Kinderconsument, a Dutch consumers' organization for children, published their own sampling study among 1300 children from 10 to 13 years of age. The results were alarming. Up to 44% of the children – depending on the Chat Rooms they frequented – were bothered by floods of abuse and sexual intimidation. The children were also disgusted to find that annoying men who turned out to not be children at all flooded them with abusive comments and words. They received unwanted pornographic pictures online, along with invitations to meet in person. Moreover, there seemed to be gender differences in terms of coping with the stress in Chat Rooms. Girls admitted to experiencing emotionally complex and disturbing situations on the Internet, but they tended not to tell their parents. Some even admitted to having an online love affair—without their parents knowing about it (Benschop, 2003).

In other jurisdictions around the globe, tougher laws – similar to those found in the United States and Canada – have recently been passed. They are aimed at curbing child pornography, because of the harm that such portrayal and ensuing violent acts inflict on innocent parties. For example, in South Africa, the Film and Publications Act has recently been amended, such that those who breach the Act – producing, distributing, and possessing child pornography – face up to 30 years behind bars. Also, large companies could also face prosecution if their employees are caught with child pornography in their emails or attachment folders thought to have been deleted, and ISPs could face criminal prosecution if they fail to block access to child porn Websites after members of the public or the police have told the ISPs of the sites' existence. Moreover, individuals repairing computers could be held criminally liable if they do not report clients whose computer hard drives contain pornography. The same outcome would apply to photography on films sent in for developing and printing (Ajam, 2004).

Also, in late 2005, the EU Council of Ministers adopted a Framework Decision on combating trafficking in human beings and on combating the sexual exploitation of children and child pornography. With a 45 million Euro budget from 2005 to 2008, the draft program would fund projects to protect children against harmful content, including the extension of an existing network of national hotlines to cover more European countries. New member states and candidate countries were especially targeted, as no hotlines currently exist in these countries. The development of filtering technologies was also to be encouraged under the program but with due respect to EU privacy rules. The Commission is to report by mid-2006 on the implementation and effectiveness of the program (EurActiv, 2005; EUROPA, 2006).

It should be mentioned that in 1989, the UN Convention on the Rights of the Child became the first legally-binding international instrument to incorporate the full range of human rights—civil, cultural, economic, political and social rights. Back then – even before the massive growth in child porn on the Internet – world leaders decided that children needed a special convention against abuse, and they wanted to make sure that the world recognized that children – as well as adults – have human rights. The Convention sets out these rights in 54 articles and two Optional Protocols, and it defines the basic human rights that children everywhere have: the right to survival; the right to develop to the fullest; the right to protection from harmful influences, abuse and exploitation; and the right to participate fully in family, cultural and social life (UNICEF, 2006).

The four core principles of the Convention are non-discrimination; devotion to the best interests of the child; the right to life, survival and development; and respect for the views of the child. Every right spelled out in the Convention is inherent to the human dignity and harmonious development of every child. The Convention protects children's rights by setting standards in health care; education; and legal, civil and social services. By agreeing to undertake the obligations of the Convention, national governments commit themselves to protecting and ensuring children's rights. Equally important, they have agreed to hold themselves accountable for this commitment before the international community (UNICEF, 2006).

1.18. A summary of whether online child porn legislation is working

So, does online child porn legislation appear to be working? In a report released on April 20, 2005, on children as victims of violent crime, the office of Statistics Canada said that charges related to child pornography increased eight-fold over the period from 1998 through 2003. The increase in charges laid by law enforcement agents in Canada has been the result of several factors—including increased public awareness about the potential of the Internet to cause harm to children, police having increased and proper resources to conduct the investigations, improved laws having "the teeth" to charge cyber pornographers, and improvements in technology for catching the cyber criminals in their acts. Also, volunteers like the CyberAngels and online citizens patrolling the Internet for cyber criminals and then advising the proper authorities has aided in their capture.

However, as lawmakers keep reminding its citizens, cyber child porn, like cyber crime, in general, is difficult to control because by its very nature, it has disrespect for national boundaries. As a report prepared by McConnell International stated, effective law enforcement is hampered by the transnational nature of cyberspace. Existing mechanisms for aiding police trying to communicate over national borders to resolve and prosecute crimes are often complex and slow. Moreover, cyber criminals are able to defy the conventional jurisdictional realms of sovereign nations by starting an attack against the principles of society from almost any computer in the world and transmitting offensive and often violent information across multiple national boundaries in a matter of seconds. Such techniques, therefore, dramatically increase both the legal and the technical complexities of investigating and prosecuting cyber crimes, including cyber child pornography (McConnel International, 2000).

It is for this reason that legal authorities are asking volunteer online communities like home PC owners and businesses to assist in fighting against heinous crimes committed over the Internet. Royal Mounted Canadian Police Corporal Jim Gillis, head of Project Horizon, a policing initiative dealing with online child pornography and based in Halifax, Nova Scotia, said that home PC owners and businesses play an unknown but key role in promoting cyber child porn criminal activities, for a large part of the problem arises from the fact that bots are often planted by a virus on home and business computers to convert them into zombies that are remotely controlled by cyber criminals. Though the computers may appear to be operating normally, they could actually be relaying child pornography traffic or storing child porn images. In this way, cyber criminals can actually avoid detection by legal authorities (Butters, 2005).

2. Using technology to curb online child pornography

Increasingly, specialized police units are working together to fight cyber crime, since, by their very nature, law enforcement agencies have narrowly-defined jurisdictions within which they are legally allowed to operate. To increase communication flow between such specialized units, as one case in point, criminal intelligence officers based in Lyons, France, moderate the Interpol Internet workstation, where elite forces like Canadian Paul Gillespie's and Jim Gillis's specially-trained experts meet online to share information about cyber child porn rings and cyber child pornographers.

2.1. How software technology assisted police in detecting a March, 2006, international cyber child porn ring

In March, 2006, this meshing of cyber intelligence had a major payoff. A tip to authorities from an Edmonton, Alberta, woman who overheard Canadian children talking about sexual abuse, coupled with the creative cyber-sleuthing expertise of the Toronto, Ontario, police sex crimes unit led to the investigation of an online Chat Room that resulted in the arrests of 27 men in an international child porn ring on March 16, 2006.

The cyber child porn ring used the Internet to share violent and degrading homemade child porn, including images of some men raping their own children—some under age 12 and one fewer than 18 months in age. U.S. Attorney-General Alberto Gonzales told a news conference that the international undercover investigation disclosed an insidious network of men engaged in worldwide child porn trafficking. At the time of the ring's announcement, Canadian police arrested nine men. Thirteen suspects were charged in the United States, three suspects were charged in Australia, and two were charged in the United Kingdom. The charges included possession of child porn, and the receipt, distribution, and production of photos and live-streaming videos of adults sexually abusing minors. The project commenced in May, 2005, after the women contacted the Edmonton, Alberta, Internet child exploitation unit. Detective-Sgt. Paul Gillespie of the Toronto, Ontario, unit said that pedophiles tend not to respect geographical borders, so why should the sex crime units? He added that whether the child who is being abused resides in Toronto or anywhere else, it is the sex crime unit's job – regardless of its worldwide geographic location – to rescue children from such violence (Sher, 2006).

The Edmonton, Alberta, Canada, man who was the individual abusing his own stepchildren out West and posting the abuse on the Internet was reported by the woman to police after overhearing the children talk about the abuse. The man was arrested by Canadian police, was found guilty of the charges, and received a sentence of 14 years in prison. He told police that he was in contact with several men using an Internet P2P (Peer-to-Peer) software called WinMX to coordinate their file-sharing activities. However, since the recent crackdown against illegal music and other illegal file downloading on the Net, in contravention of the Digital Millennium Copyright Act (DMCA) of 1998, many of the cyber child porn perpetrators were forced to commit their acts on the fringes of the World Wide Web—thus making their acts harder to monitor by police (Sher, 2006).

The Edmonton pedophile identified two Chat Rooms as regular venues for the exchanges: Kiddypics and Kiddyvids. Police said that the Chat Rooms were difficult to investigate for a number of reasons. First, they were run by a tightly-knit group of administrators. Second, the pedophiles used nicknames to disguise their identities. Third, the pedophiles used a complicated system to shield their Internet Protocol (IP) addresses (a type of digital signature that every computer acquires when it logs on to the Net—and can assist police in the identification of an Internet user's location). Because of the information-sharing capability between police in various jurisdictions, the second break in the case came when Canadian police contacted U.S. police and told them that one of the men on the "buddy list" of the charged Edmonton man apparently was from Chicago—an abuser of his infant daughter (Sher, 2006).

A major breakthrough came in the case when Chicago police investigators could identify the code hiding the IP address of the key Chat room administrator—an Edmonton, Alberta, shipping clerk by the name of Carl Treleaven, aged 49. When the police arrived at Treleaven's home and seized his computer – containing 20 gigabytes of child porn – 90 people around the world were waiting for child porn downloads. Treleaven was not new to police; he was arrested in 1986 for indecent assault and in 1993 for gross indecency. In the latest incident, the judge hearing the case sentenced him to 3.5 years in prison (CBC News, 2006a,b; CBC News, 2006b).

Police in Canada and the rest of the world were assisted in sharing vital information regarding this case with special Microsoft, Inc. software known as the Child Exploitation Tracking System (CETS)—which works as a secure, internal search engine for specially-trained cyber porn investigators. Using this software, police can run queries for information stored in computers around the globe—including suspects' online monikers, the names of Chat Rooms, and online addresses. These CETS terminals are currently operational in a number of Canadian jurisdictions, and they are at various stages of deployment in the United States, Italy, Brazil, Australia, and Indonesia (Sher, 2006).

It is noteworthy that in recent years, companies like Microsoft, Inc. have decided to help authorities fight cyber child pornographers. CETS has an interesting history. One day in 2003, disgusted by the lack of cooperation the police were receiving from large high-tech companies, Toronto's Det.-Sgt. Paul Gillespie emailed Bill Gates. He told Mr. Gates that the Internet was facilitating an explosion in child pornography, making it much easier for the culprits to escape detection. He said that his elite team of experts was falling behind, he was personally frustrated at the obstacles he faced, and he needed the expert help found at Microsoft. To Gillespie's surprise, Mr. Gates responded affirmatively (Morgan, 2006).

Within weeks, Microsoft, Inc., Gillespie's experts, and the Royal Canadian Mounted Police (RCMP) formed a team—which eventually produced the $4.5 million software program called CETS. Besides the most recent March, 2006, case, this software has led to a number of arrests, because it allows police forces to work together more effectively, searching for and exchanging encrypted information about offenders and victims. This so-called cutting-edge social-network-analysis feature assesses large amounts of information and assigns scores to individuals appearing to be more active on child porn viewing and distributing than officers might have otherwise thought. While about twelve countries have so far expressed interest in adopting CETS technology (including those listed above), the end goal is that all countries will be connected, including those in the developing countries where the child-sex tourism and exploitation problems flourish (Morgan, 2006).

2.2. Why new technological approaches are needed to fight cyber child porn

The evidence presented thus far in this review paper underscores the importance and urgency of combating cyber child pornography—by home PC users, the police, the courts, and corporations. Until the advent of software such as CETS, most of the cyber child porn combat focus had been on legal measures passed by various countries to curb this disturbing and violent cyber crime. However, because of differing definitions of what is purported to be illegal in various jurisdictions around the globe, the police and prosecutors have found it exceedingly difficult to produce a coordinated and compelling evidence case to put many child porn perpetrators behind bars (BBC News, 2001c).

Moreover, differences in definition of what actually constitutes child porn have meant that different jurisdictions have resulted in different interpretations of the crime—and related punishments and remedies. Consequently, in some jurisdictions, a cyber child pornographer may get only three or four years behind bars, while in other jurisdictions, a perpetrator may be behind bars for life. In short, child porn legislation around the globe differs according to age of consent, form of content, fictitious/non-fictitious portrayals of sexual activities, attribution, and other key factors. Adding the virtual world of the Internet to the legal picture has complicated the issue even further over the past six years. Too, there is no central governing judiciary body for combating cyber child porn, and some jurisdictions – such as those in Europe – have a more liberal interpretation of what constitutes child porn.

Furthermore, by default, the Internet provides a certain level of anonymity to users engaged in online child-porn sharing. While there are increasingly effective methods for discovering the online identities of individuals, heavy encryption and/or encrypted Peer-to-Peer (P2P) networks exacerbate the problem. Since the current legislative and logistical problems present a sizable barrier that must be overcome if child pornographers are to be stopped in their tracks, a network infrastructure approach to combating the problem may prove to be significantly more efficient at detecting offensive material being transmitted over the Internet.

The balance of this review paper explores solutions based on technical methods that allow for the efficient detection of child pornography on the Internet. The authors believe that the problem of combating child porn on the Net can be approached effectively using adapted network infrastructure security solutions for detecting malicious traffic. Without question, detecting child porn at the network level using "any" traffic filter or classifier is not a trivial task, for there is much evidence of arduous ongoing efforts to achieve effective traffic classification at the network level. Before detailing our proposed approach of using Bloom filters with counters and a novel classifier that combines the principles of a recently-proposed weak estimator and a linear classifier aimed to speed-up the classification stage (Chopra, VargasMartin, Rueda, & Hung, in presss-a, Chopra, VargasMartin, Rueda, & Hung, in press-b), we will discuss a number of host and network-based approaches to assist in combating child pornography.

2.3. Host-based approaches

A related area to child pornography detection is content-based image and video retrieval, or CBIR. This area has become more important with the emerging, increasing use, and sharing of digital visual (image and video) files. The associated complexity of the problem is to be able to retrieve visual files based on their semantics. The semantics of a file are determined according to a set of characteristics (e.g., color contrast and shapes) learned a-priori from similar files. Image and video retrieval techniques are already being proficiently exploited and have been extensively studied (Bajai, Inc., 2005; Kherfi, Ziou, & Bernardi, 2004).

Applications that have driven CBIR development have included combating child pornography, but there is still much room for improvement in terms of the reliability of this method. A number of jurisdictions have been working on improving this method. For example, the Swedish National Police have created a database of patterns to be used with CBIR that is to be shared with other European countries. The databases are most often populated through content captured in child porn raids or downloaded from the Internet. While work in this area is, indeed, promising the consensus among experts is that a lack of established or negotiated standards for forensic image management is hampering its progress (Lynn, 2004).

The CBIR method has been used to match pictures taken within the same environment to identify the origin of the material. While CBIR can potentially be combined with "white worms" – which can scan the Internet in search of child pornography and report suspicious content to law enforcement – this technique has affiliated legal implications that have proven to be controversial across jurisdictions in the recent past (Tanase-Avatavului, 2005).

Finally, host-based solutions like parental controls have in the past been faulty, but they are continuously improving and they are becoming increasingly visible features within newer operating systems, such as Apple Computer's latest version of Mac OS X. A popular approach to using parental controls is to begin by "white-listing" sites and contacts that parents want their children to access. As the child matures, the parents may move to "black-listing" sites that they do not want their children to access. Another commonly suggested path advocated by experts is to educate children about making responsible choices on the Internet to protect themselves against cyber criminals. This approach is often linked to social awareness programs aimed at educating society as a whole about evil forces lurking on the Net. While such host-based and social education program solutions are useful, they do suffer limitations. Not all hosts are accessible or open to scanning, and many parents do not know how to enable parental controls or other online safeguards (Aiken, 2002).

The authors propose that a network infrastructure approach could overcome many of these issues.

2.4. Censured Peer-to-Peer (P2P) traffic approaches

While a number of P2P program vendors have entered alliances to combat child porn, most programs used for file sharing are not in any way part of such an alliance (Borland, 2004). Moreover, the state of P2P programs is rapidly changing to include heavy encryption and anonymity features. One of the largest of these networks is facilitated by a program called "Share," which is one of the most popular P2P programs in use in Japan.

There is little question that the P2P field enjoys much attention within research circles, and it is conceivable that it may become a primary distribution point for child pornography in the future. Features such as censorship-resistant publishing make it possible to anonymously and systematically distribute sets of files on networks—an environment that can be abused for malicious purposes. The problem presented by the P2P field has different possible approaches, for the various P2P protocols in existence have different methods for uploading or downloading material from the Net. As such, targeting any single P2P network requires detailed knowledge of the protocol in use. Network infrastructure techniques can be developed to analyze traffic without knowing the overlying protocols or the specifics of networks, such as the ones created by P2P applications. Moreover, any solution targeted at a specific protocol, application, or network will have limited applicability and likely decreasing utility as offenders move to new ways of distributed child pornography online.

It is important to consider the case of anonymous and encrypted file P2P applications, such as Winny (Wikipedia, 2006). These applications introduce additional complexity for the detection and identification of cyber porn, for encrypted payloads tend not to be susceptible to CBIR or email surveillance techniques. Recently, researchers Ohzahata, Hagiwara, Terada, and Kawashima (2005) have presented useful identification mechanisms based on the Transport Control Protocol (TCP) handshake behavior. Their system resides inside an autonomous system and is, therefore, capable of detecting encrypted P2P file transfers. In short, attribution of anonymous P2P nodes at the network infrastructure level is challenging, and it is a problem that has yet to be effectively addressed.

2.5. Network-level approaches

Many child pornography images are found through underground Web sites on the Internet. In fact, many newsgroups are devoted to child pornography, with names such as "alt.pictures.binary.pedofile" or "alt.pictures.erotica.dhildren."

A number of network-level approaches exist for combating child pornography. These technical approaches can be classified within a traffic-type model that consists of visual-, text-, and encrypted-type traffic. Visual-type traffic consists of moving pictures or frames. Subclasses of this type are still pictures, such as JPEG files. These files are typically transferred over the Internet using P2P applications. Text-type traffic consists of items like emails and documents, and includes descriptions of child pornography and suspicious material such as Chat Room sessions, whereby one online user inquires about another online user's age. Finally, encrypted file-transfers represent an even more challenging scenario, because it may be computationally unfeasible to analyze encrypted file contents.

In a typical approach to detecting child pornography on the Internet, law enforcement officers conduct manual searches on the Internet, or use the Internet to establish contact with offenders to make arrests and to remove censured content. As noted earlier in this paper, this host-based approach is resource intensive and is very inefficient. Implementing detection mechanisms in internal network equipment may not be as effective as implementing them in the network infrastructure equipment—which can inspect larger volumes of traffic originating from different networks.

In particular, we are focusing our efforts on finding ways in which censured material can efficiently be identified. We believe that network security mechanisms can serve this purpose if appropriately adapted. In short, the idea is to enable routers of the network infrastructures to detect child pornography files along the communication channels and to possibly identify suspect network segments involved in this illegal file transfer. This proposed system should be able to trace offending material using core routers—an approach which differs significantly from the host-based, manpower-intensive approach typically employed by law enforcement nowadays, whereby computers of suspected individuals are locally or remotely scanned by police for evidence of censured content using a variety of forensic techniques.

While there is a number of commercial products that can classify visual file content, such as the Bajai, Inc. products, intermediate routers may not be able to analyze visual files online for a number of reasons—including fragmentation and performance constraints.

It is important to realize that information is passed along the Information Highway from host to destination not as entire pieces of data but in information packets that are disassembled and reassembled. When the data to be transferred over the Net exceed a predefined maximum packet size, the data are fragmented into smaller Information Protocol (IP) packets, which are reassembled at the destination end. Routers do not perform packet reassembly; therefore, intermediate routers participating in a visual file transfer may not see the whole visual file within a single packet. Regarding performance constraints, visual files classification is time-consuming and routers may not be able to cope with high volumes of traffic.

We authors believe that with appropriate adaptations, some filtering and efficient classification techniques used to detect malicious code at the network level can be useful in more effectively and efficiently combating child porn in unencrypted text, image, or video formats.

2.6. The proposed classifier for dealing with non-stationary data like cyber child porn

As previously noted in this paper, all of the existing classification systems suffer from the inability to capture quick changes in the distribution of the source data, such as when dealing with non-stationary data like cyber child porn. First, let us assume that the input data comes in IP packets of a small size, say 512 bytes, and from different sources, say from different types of scenarios—as what typically occurs during the exchange of documents, child porn or otherwise. Second, let us assume that these IP packets originated from different applications. Third, let us assume that we are using a classifier that characterizes the data by means of their statistical distribution. Dealing with statistical distributions of the data implies the use of estimators, as the actual distribution is typically not known. To estimate the parameters of the underlying distribution in this scenario, the estimator has to be capable of "learning" these parameters to quickly detect their changes.

Quite a few of the estimators have been shown to be robust, such as the maximum likelihood estimates, or MLE, and the Bayesian estimates (Duda, Hart, & Stork, 2000). These estimators, though robust in the sense that they possess many asymptotic convergence properties, have not been able to cope with the problem of changing distributions, or even their parameters. Even the use of a "window" to estimate the MLE parameters has not been the best option, since it is difficult to determine in advance the width of such a window.

To deal with this kind of estimation problem, Oommen and Rueda (2004) recently proposed a stochastic learning-based weak estimator, or SLWE. The SLWE has been successfully used to deal with problems involving non-stationary data. One of these kinds of problems deals with adaptively compressing data files containing text (like Word files) interspersed with mathematical formulas, pictures, and tables. In this context, the SLWE used in combination with traditional adaptive encoding techniques has been shown to compress nearly 10% more of the data files than traditional estimators are able to compress (Rueda & Oommen, 2004).

Another scenario involving non-stationary data consists of classifying news streams coming from different sources and that keep changing with time. An example of the latter would be news of different types broadcast on television or accessed through the Internet. Oommen and Rueda (2005) have recently shown that the SLWE, coupled with a fast linear classifier, achieves high classification accuracy on detecting different sources of television news, sports, and business reports, based on the adhered closed-captioning text for the hearing impaired.

Based on these recent studies, the authors propose using a classifier combining the SLWE and a linear classifier. Our justification is based on these points: First, the data come in IP packets of 512 bytes (drawn from a source alphabet). Second, the IP packets belong to one of two classes: obscene and non-obscene. Third, the source alphabet contains n symbols for the image files ($n=256$)—conforming to the realizations of a multinomial random variable and whose estimates are updated using SLWE rules. While the authors accept that different rules can be used, we submit that since we want to capitalize on speed of classification, we are proposing using the linear multiplicative rule, akin to the family of linear-reward-action probability schemes. While this rule requires a "learning" parameter, λ, it has been reported that a good value for multinomial scenarios should be close to 1 (Oommen & Rueda, 2005).

For the next stage, the authors submit that the estimated probabilities of the source symbols should be used to feed a linear classifier as follows. At time 'k,' the estimates obtained from the SLWE at time '$k-1$' conform to a d-dimensional vector; namely, the feature vector associated with the kth symbol, x_k. The linear classification rule consists of a simple algebraic operation $w^t x_k + w_0$, where w and x_k are $d \times 1$ matrices and where w_0 is a threshold weight. Each symbol is classified, and the whole packet is assigned to the class with the largest number of symbols belonging to it. Note that it is also possible to group IP packets in such a way that the whole group could be assigned to the same class.

On the other hand, the algebraic operation $w^t x$, usually called *dimensionality reduction*, is aimed at finding a vector w (or a matrix, in a more general case) that efficiently classifies the data in the reduced space – of one dimension, in our case – and by means of a new classifier—the threshold w_0, in our case.

Quite a few techniques have been proposed for finding w, with the most well-known methods being the *perceptron algorithm*, the *minimum square error classifier*, *Fisher's classifier*, and the *Chernoff-distance-based LDR technique*. Moreover, the value of w_0 can be found in different ways, or another multi-dimensional classification task can be performed in the reduced space. When the latter is of dimension one, the algebraic operation $x_k + w_0$ result in a value, where positive implies x_k and is assigned to class obscene, and where negative implies x_k and is assigned to class non-obscene. Ties are resolved arbitrarily (Loog & Duin, 2004; Rueda, 2004).

Our dataset consists of a significantly small number of IP packets drawn from the transmission of pictures over the Internet using an unencrypted communication protocol and belonging to one of two classes: obscene and non-obscene. We are currently designing tests with "sanitized" (i.e., pictures having blurred silhouettes) child pornography pictures provided by the Toronto, Ontario, police unit.

To validate and assess the quality of the classifier, we will apply the m-fold cross-validation approach (Duda et al., 2000) and compute the mean and standard deviation of different measures, including *sensitivity*, *specificity*, and *accuracy*. The classification rule will be validated using labeled IP packets (for which the class is already known), and adjustments will be done, if necessary. Note, however, that in the actual classification process, the label of each IP packet is unknown.

For the reasons discussed above, and due to the nature of the data to be classified, we expect that the proposed classification system will be capable of classifying IP packets containing textual or visual child pornography—thus assisting in the arrest and prosecution of cyber child pornographers.

2.7. The source address reputation system

The authors also propose a source IP address reputation system that will keep an *obscenity-score* for each source IP address, which increases the likelihood of a positive result regarding a transmitted (obscene or otherwise) IP packet (see Weaver, Staniford, & Paxon, 2004). The system will determine whether a given IP address has been transferring obscene material in the recent, past based on a given obscenity score. Furthermore, packets may be traced back using a simple source IP address trace-back or some other more sophisticated approach (such as that described by Snoeren et al., 2001).

Given constraints on performance and memory capacity, it may be difficult for routers of the network infrastructure to keep track of the *obscenity-score* of every single IP address transmitted in the recent past. To overcome this potential barrier, we propose using Bloom filters with counters (BFWC). A Bloom filter is a hash-based method for testing membership of a series of items in a large given set of items, with allowable errors (Bloom, 1970). Fan, Cao, Almeida, and Broder (1998) introduced BFWC applied to Web cache techniques.

We propose to enhance the routers of a network with BFWC to analyze outbound traffic. For each outbound packet p classified as *obscene*, an *enhanced router* (i.e., a router that implements a BFWC and the classification system) increments the *obscenity-score* of the corresponding source IP address—such that the obscenity scores will be re-set to 0 every time period r. If the *obscenity-score* of this source IP address exceeds a maximum tolerable value t (the behavior prototypical of pedophiles accessing cyber child porn), an alarm would be triggered, thus notifying experts that a likely perpetrator has been found.

The expected number of false alarms triggered by a BFWC depends on r, and t, and other parameters addressed by Van Oorshot, Robert, and VargasMartin (in press). In closing, we believe that our classification system with a BFWC adjusted for appropriate parameters is promising as a technique that will assist law enforcement in detecting cyber child pornographers, and we fully expect to report positive test results in future papers.

3. Conclusion

Differences in the definition of cyber child pornography have been complicating the prosecution of cyber child pornographers around the globe, and the reality is that jurisdictional problems will likely continue for a while longer. Recent international efforts of experts trained in cyber child porn detection and coalitions formed that encompass wider geographic ranges may enable law enforcement agencies to work together more effectively to curb this heinous and violent crime.

Clearly, combating the problem of cyber child porn requires a multi-faceted defense—including balancing citizens' freedom of speech with causing intended violence to minors, educating the likely targets (children and women) in society about protecting themselves while interacting online, and developing technological approaches for identifying online child pornographers. As noted in this review paper, the area of network infrastructure techniques applied to this particular problem remains largely unexplored.

Our technical approach to combating cyber child pornography consists of enhancing routers with a classification system combining the SLWE with a linear classifier. This classification system, along with a Bloom filter with counters which keep track of source IP address reputation, will be tested using "sanitized" data sets provided by the Toronto, Ontario, police department. The results are expected have a positive outcome and will be reported in future papers. We also believe that the proposed system can be used in other areas such as Homeland Security.

References

Adams, C. (2004). In M. D. Smith (Ed.), *Pornography: Encyclopedia of rape.* Westport, CT: Greenwood Publishing.

Aiken, J. (2002, May 2). *Report: No one fix for net porn and kids.* Retrieved March 20, 2006, from http://cnnstudentnews.cnn.com/2002/TECH/internet/05/02/youth.internet.porn/

Ajam, K. (2004, September 26). *Tough new measures to fight child porn.* Retrieved March 14, 2006 from http://www.crime-research.org/news/26.09.2004/664/

BBC News (2001, March 26). *International child porn ring smashed.* Retrieved March 10, 2006, from http://news.bbc.co.uk/1/hi/world/americas/1244457.stm

BBC News (2001, August 8). *U.S. breaks child cyber-porn ring.* Retrieved March 11, 2006, from http://news.bbc.co.uk/1/hi/world/americas/1481253.stm

BBC News (2001, November 14). *Child porn raids in 14 countries.* Retrieved March 14, 2006, from http://news.bbc.co.uk/1/hi/world/europe/1656779.stm

Bajai, Inc. (2005). Bajeye version 5. Retrieved March 20, 2006, from http://www.bajai.com/home.html

Benschop, A. (2003, August). *Child pornography in cyberspace.* Retrieved February 3, 2006, from http://www2.fmg.uva.nl/sociosite/websoc/pornography_child.html

Bloom, B. (1970). Space/time trade-offs in hash coding with allowable errors. *Communications of the ACM*, *13*, 422–426.

Borland, J. (2004, December 12). *P2P group launches site to combat child porn.* Retrieved March 20, 2006 from http://news.com.com/P2P+group+lauches+site+to+combat+child+porn/2100-1025_3-5488290.html

Brenner, S. (2001, June). *Is there such a thing as 'virtual' crime?* Retrieved February 1, 2006 from http://www.crime-research.org/library/Susan.htm

Butters, G. (2005, January 27). Criminal activity: Your computer may be housing child porn. *The Globe and Mail*, B14.

CBC News (2003, November 5). *The fifth estate: Landslide.* Retrieved March 10, 2006, from http://www.cbc.ca/fifth/landslide/resources.html

CBC News (2003, November 5). *The fifth estate: Landslide: Profile of a pornographer.* Retrieved March 11, 2006, from http://www.cbc.ca/fifth/landslide/profile_printer.html

CBC News (2006, March 8). *Edmonton man awaits sentencing in child porn case.* Retrieved March 19, 2006, from http://www.cbc.ca/calgary/story/ca-child-porn20060308.html

CBC News (2006, March 17). *Man at centre of child porn case gets 3-and-one-half years.* Retrieved March 20, 2006, from http://www.cbc.ca/calgary/story/ca-treleaven20060317.html

Chopra, M., VargasMartin, M., Rueda, L., & Hung, P. (in press-a). Toward new paradigms to combating Internet child pornography. *Proceedings of the Canadian Conference on Electrical and Computing Engineering (CCECE '06)*, IEEE Canada, Ottawa, Ontario.

Chopra, M., VargasMartin, M., Rueda, L., & Hung, P. (in press-b). A source address reputation system to combating child pornography at the network level. Proceedings of the IADIS International Conference on Applied Computing. San Sebastian, Spain.

CyberAngels (2005). *CyberAngels.* Retrieved March 10, 2006, from http://www.cyberangels.org/

Department of Justice Canada (2002, June 10). *Highlights of Bill C-15A: An act to amend the Criminal Code and to amend other acts protecting children from sexual exploitation.* Retrieved March 11, 2006, from http://canada.justice.gc.ca/en/news/nr/2002/doc_30531.html

Duda, R., Hart, P., & Stork, D. (2000). *Pattern classification* (2nd ed.). New York: John Wiley and Sons.

EurActiv (2005, November 14). *EU to crack down on internet child porn and junk emails.* Retrieved March 14, 2006, from http://www.euractiv.com/Article?tcmuri=tcm:29-133242-16 and type=News

EUROPA (2006). *EU action against trafficking in human beings and the sexual exploitation of children.* Retrieved March 14, 2006, from http://europa.eu.int/comm/justice_home/fsj/crime/trafficking/fsj_crime_human_trafficking_en.htm

Fan, L., Cao, C., Almeida, J., & Broder, A. (1998). Summary cache: A scalable wide-area web cache sharing protocol. *IEEE/ACM Transactions on Networking*, *8*, 281–293.

Frieden, T. (2002, May 1). *New child porn measure announced.* Retrieved March 14, 2006, from http://cnnstudentnews.cnn.com/2002/LAW/05/01/ashcroft.child.porn/

Karp, H. (2000, April). Angels on-line. *Reader's Digest*, *157*, 50–56.

Kherfi, M., Ziou, D., & Bernardi, A. (2004, March). Image retrieval from the world wide web: Issues, techniques, and systems. *ACM Computing Surveys (CSUR)*, *36*, 35–67.

Lai, T. (2005, August 11). Ajax pastor charged with luring child for sex. *The Globe and Mail*, A9.

Loog, M., & Duin, R. (2004). Linear dimensionality reduction via a heteroscedastic extension of LDA: The Chernoff criterion. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, *26*, 732–739.

Lynn, C. (2004). *Image recognition takes another step forward.* Retrieved March 20, 2006, from http://www.seyboldreports.com/TSR/subs/0417/image_recognition.html

Magid, L. (2002, March 21). *Net users can help fight child porn.* Retrieved March 9, 2006, from http://www.pcanswer.com/articles/sjm_childporn.htm

Mashima, R., & Hirose, K. (1996, September). *From "dial-a-porn" to "cyberporn": Approaches to and limitations of regulation in the United States and Japan.* Journal of Computer-Mediated Communication online Retrieved March 10, 2006, from http://jcmc.indiana.edu/vol2/issue2/mashima.html

McAuliffe, W. (2001, August 9). *Commercial child porn ring bust leads to 100 arrests.* Retrieved March 14, 2006, from http://news.zdnet.co.uk/internet/0,39020369,2092866,00.htm

McCafferty, C. (2004). *Only we can tackle porn.* Retrieved March 14, 2006, from http://www.christianaction.org.za/articles_ca/2003-3-Only_We_Can.htm

McConnel International (2000, December). *Cybercrime…and punishment? Archaic laws threaten global information.* Retrieved March 11, 2006, from http://www.mcconnellinternational.com/services/cybercrime.htm

McIlroy, A. (2005, October 31). Cyber ghosts and email from the dead. *The Globe and Mail*, A3.

Miltner, K. (2005, May). *Discriminatory filtering: CIPA's effect on our nation's youth and why the Supreme Court erred in upholding the constitutionality of the Children's Internet Protection Act.* Retrieved February 2, 2006, from http://www.findarticles.com/p/articles/mi_hb3073/is_200505/ai_n15014919

Morgan, R. (2003). *Sisterhood is forever: The women's anthology for a new millennium.* New York: Washington Square Press.

Morgan, J. (2006, March). ruinyrpjs? Reader's Digest, 168, 131–132, 134–140.

Ohzahata, S., Hagiwara, Y., Terada, M., & Kawashima, K. (2005, March 31-April 1). A traffic identification method and evaluations for a pure P2P application. *Proceedings of Passive and Active Networks Measurement Workshop, Boston, Massachusetts* (pp. 55–68). Retrieved March 20, 2006 from http://www.informatik.uni-trier.de/~ley/db/conf/pam/pam2005.html

Oommen, B., & Rueda, L. (2004). A new family of weak estimators for training in non-stationary distributions. *Proceedings of the Joint IAPR International Workshop on Statistical Pattern Recognition* (pp. 644–665). Lisbon, Portugal.

Oommen, B., & Rueda, L. (2005). On utilizing stochastic learning weak estimators for training and classification of patterns with non-stationary distributions. *Proceedings of the 28th German Conference on Artificial Intelligence* (pp. 107–120). Koblenz, Germany.

Posey, J. (2005, December 29). *Child pornography: Is it so bad?* Retrieved February 2, 2006 from http://www.pedowatch.com/porn.htm

Ropelato, J. (2005). *Internet pornography statistics.* Retrieved March 10, 2006, from http://internet-filter-review.toptenreviews.com/internet-pornography-statistics.html

Rueda, L. (2004). An efficient approach to compute the threshold for multi-dimensional linear classifiers. *Pattern Recognition*, *37*, 811–826.

Rueda, L., & Oommen, B. (2004). On families of new adaptive compression algorithms suitable for time-varying source data. *Proceedings of the Third Biennial International Conference on Advances in Information Systems* (pp. 234–244). Izmir, Turkey.

Schell, B., & Martin, C. (2004). *Contemporary world issues: Cybercrime.* Santa Barbara: ABC-CLIO.

Sher, J. (2006, March 16). Police bust worldwide child-porn ring. *The Globe and Mail*, A7.

Snoeren, A., Partridge, C., Sanchez, L., Jones, C., Tchakountio, F., Kent, S., et al. (2001). Hash-based IP traceback. *Proceedings of the ACM SIGCOMM Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication (SIGCOMM '01)* (pp. 3–14).

Tanase-Avatavului, M. (2005). Shape decomposition and retrieval. Doctoral Thesis, University of Utrecht. Retrieved March 20, 2006, from http://www.cs.uu.nl/groups/AA/multimedia/publications/pdf/mindshade.pdf

Uebel, M. (2002, May 31). *Toward a symptomatology of cyberporn.* Retrieved March 14, 2006, from http://muse.jhu.edu/journals/theory_and_event/v003/3.4uebel.html

UNICEF, M. (2006). *Convention on the rights of the child.* Retrieved March 14, 2006, from http://www.unicef.org/crc/index.html

U.S. Department of Justice (2003, April 30). *Fact sheet. PROTECT Act.* Retrieved February 2, 2006, from http://www.usdoj.gov/opa/pr/2003/April/03_ag_266.htm

Van Oorschot, P. Robert, J-M., & Vargas Martin, M. (in press). A monitoring system for detecting repeated packets with applications to computer worms. *International Journal of Information Security.*

Weaver, N., Staniford, S., & Paxon, V. (2004, May 17). *Very fast containment of scanning worms.* Retrieved March 21, 2006, from http://www.icsi.berkeley.edu/~nweaver/containment/

Wikipedia. Winny. Retrieved March 20, 2006, from http://en.wikipedia.org/w/index.php?title=Winny and oldid=31980964