

PERSPECTIVES ON THE CAPACITY  
OF THE CANADIAN POLICE SYSTEM TO RESPOND TO “CHILD  
PORNOGRAPHY” ON THE INTERNET

By

Catherine J. Dawson

Master of Education, Simon Fraser University, 1999

Bachelor of General Studies, Simon Fraser University, 1996

Associate of Arts, Camosun College, 1974

EXTENDED PAPER SUBMITTED IN PARTIAL FULFILLMENT OF  
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF ARTS

In the

School of Criminology and Criminal Justice

©Catherine J. Dawson

UNIVERSITY OF THE FRASER VALLEY

Fall 2009

All rights reserved. This work may not be  
reproduced in whole or in part, by photocopy  
or other means, without permission of the author.

## **Abstract**

The Internet, its affordability, accessibility, and anonymity provide new venues where child exploitation crimes have increased. An exponential rise in the exchange of images of sexual abuse, commonly referred to as 'child pornography', has occurred. The purpose of this major paper was to explore this phenomenon within an international context, and assess the capacity of Canadian law enforcement (national and municipal) to respond. In order to do so a survey was sent to police departments across Canada, to have officers identify the challenges they faced in responding to images of child abuse on the Internet, and to solicit officers' general opinions on this issue. The research resulted in five key findings that implied that existing capacity gaps were rooted in a lack of applied or ratified international agreements and commitments, a failure of system interoperability, a lack of effective private-public partnerships, and the weaknesses in current Canadian legislation, particular to mandated reporting of suspicious content (which is now under review). Finally, a lack of appropriate, accessible support and training for police was identified. Informed by the research, the author makes several recommendations.

## **Acknowledgements**

The author wishes to thank the MA committee members Dr. Darryl Plecas and Dr. Irwin Cohen. In addition, I would like to acknowledge the generous contributions of Deputy Chief Constable Stuart Hyde, LLB., Cumbria Police, (United Kingdom), Chief Superintendent Richard Bent, RCMP E-Division, Vancouver, and Chief Constable Lorne Zapotichny, New Westminster Police Service. Finally, I would like to thank Suzanne Veit for her translation services.

## **Dedication**

This work is dedicated to the memory of my parents, Eric J., and Thelma M. Dawson.

## Table of Contents

<b>Introduction</b>	1
Legal Context	3
Pervasiveness of the Crime; Impact of the Internet	10
Offenders' Use of the Internet	14
Victimization and Nomenclature	17
Challenges in Policing the Crime	20
<b>Chapter One: Literature Review</b>	23
Expertise, Technology and Training	24
A Paucity of Data	27
Police Priority Setting and Budget Impacts	29
Legislative Gaps	31
Cooperation and Capacity across Borders	34
The Canadian Response	35
<b>Chapter Two: Methodology and Results</b>	39
Methodology	39
Research Results	41
<b>Chapter Three: Recommendations to Improve Canada's and the International Communities' Capacity to Respond to the Crime of Child Pornography on the Internet</b>	51
<b>Chapter Four: Conclusion</b>	84
<b>References:</b>	88
<b>Appendix 1: Letter of Request</b>	97
<b>Appendix 1: Survey Document</b>	98

## **Introduction**

The growth and pervasiveness of child pornography, facilitated by the Internet, has been nothing short of extraordinary. The ubiquity of the Internet, its accessibility, and its relative anonymity has created new opportunities for the collection and distribution of illegal materials. These are not simply 'dirty pictures'; police officers report that images of child abuse are getting more and more violent, and that the children in these images are getting younger (NOVOC, 2009:2). Many of the still images show severe vaginal and anal assault against young children and toddlers, and some video clips portray oral, vaginal, and anal penetration of children while in bondage (Cooper: 2006). Notably, the Behavioural Analysis Unit at the Child Exploitation and Online Protection Centre (CEOP) in the United Kingdom reported that the proportions of those who are interested in sadistic sexual acts with children are greater than previously recognized (CEOP, 2008).

Police view each image or video as visual evidence of a sexual assault of a child designed for distribution to paedophiles around the globe. However, there is evidence of the production, viewing, and distribution of this material originating in Canada. Cases in Manitoba, Quebec, and Ontario have involved children aged four, six, and nine with images of sexual assault captured digitally and distributed, as well as 'live' video clips of the abuse being committed (NOVOC,2009).

The United Nations recognized the advent of the availability of "child pornography" on the Internet over a decade ago and called for "the worldwide criminalization of the production, distribution, exportation, transmission, importation,

intentional possession and advertising of child pornography” and importantly recommended close cooperation and collaboration between Governments and the communications industry (UN: 2000). And a recent review of the literature revealed that politicians, governments, non-governmental organizations, child protection advocates, teachers, and parents everywhere demand that the police pay greater attention to this issue, solve more of these types of crimes, and rescue more children. The National Victims of Crime Advocate (NOVOC) recently released its watershed report “Every Child, Every Image” suggesting that there were over three-quarters of a million paedophiles online at any given time. That report made nine key recommendations for policy makers, the private sector, and law enforcement to eradicate images of child abuse on the Internet, and to further protect children whose sexual exploitation is facilitated by technology (NOVOC, 2008).

Regrettably, as demonstrated throughout this major paper, police in Canada and elsewhere confront serious obstacles in trying to deal with this type of crime. The barriers include police operational priorities, global legislative differences, a lack of available, current technology, and a dearth of trained personnel. Throughout the major paper, reference will be made to key capacity gaps that coalesce on these and other critical areas. The major paper will also make recommendations that are consistent with those made by leading child protection advocates and enforcement agencies who call for immediate legislative changes.

## **The Legal Context**

Child pornography is illegal in Canada and almost everywhere else. While there are no international laws with respect to child pornography on the Internet, there are a number of international organizations and agencies that influence nations with respect to both their laws and their willingness to cooperate with other countries in combating child pornography on the Internet.

At the root of international conventions, agreements, and treaties is the principle that children hold human rights and are entitled to these rights – including the right of protection from sexual exploitation. The Convention of the Rights of the Child (CRC) was adopted by the United Nations in 1989. Article 19 specifies that “States Parties shall take all appropriate legislative, administrative, social and educational measures to protect the child from all forms of physical or mental violence, injury or abuse, neglect or negligent treatment, maltreatment or exploitation, including sexual abuse, while in the care of parent(s), legal guardian(s) or any other person who has the care of the child.” Further, and more specific to images of child abuse, Article 34 requires that “States Parties shall in particular take all appropriate national, bilateral and multilateral measures to prevent the exploitative use of children in pornographic performances and materials” (United Nations, 1989).

Newell (2008) reported that the recognition of the scale of sexual exploitation has occurred primarily in the past two decades. He reported that there are now nearly thirty

international human rights instruments challenging the sexual exploitation of children including a dozen which include Europe and the Americas (Newell: 2008, 2). The three primary instruments are:

1. The UN Convention on the Rights of the Child, and the subsequent Optional Protocol on the Sale of Children, Child Prostitution and Child Photography,
2. Convention 182, the Worst Forms of Child Labour from the International Labour Organization (ILO), and;
3. The Council of Europe's convention on Cybercrime (2001) and the subsequent 2007 Convention of the Protection of children against Sexual Exploitation (Newell: 2008, 2-17).

Canada has ratified the Convention on the Rights of the Child, the Optional Protocol to the Convention of the Rights of the Child on the Involvement of Children in Armed Conflict, and the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (Library of Congress: 2007, 52).

The CRC is a broad document that speaks to the human rights and dignity of all children, and provides recommendations as well as guidelines on how to implement the convention in order to respect the rights of children. The Optional Protocol becomes much more direct in its specificity toward the sexual exploitation of children. It is now ratified by nearly 70 per cent of member UN states and speaks directly to the topic of images of child abuse. Article 3 of the protocol demands that all manner of 'child pornography', including "producing, distributing, disseminating, importing, exporting,

offering, selling or possession” is to be prohibited. Guidelines adopted later speak to the need for data collection, international assistance, and cooperation. In 2002, the CRC recommended that member states ratify the Council of Europe conventions (Newell, 2008:7).

The first Council of Europe convention, referred to by Newell as “ground breaking”, provides a global framework for international cooperation and lays the groundwork for policy development and law-making. Specifically, it also places the crime of images of child abuse within the modern, computerized context by including ‘child pornography’ on computers. The second convention extends the criminality to production, distribution and procuring or possession. The protocol calls for procedural authority for police to investigate and prosecute cybercrime offences effectively, and to provide international cooperation. While much of Canadian law reflects the principles entrenched in the Council of Europe Conventions, Canada has signed, but not ratified, this agreement.

By 2002, in a study of member EU countries, the Council of Europe discovered that even in countries that had fully ratified the Convention, few counties were entirely compliant, and many failed to implement enforcement protocols (CCJS, 2002). By 2008, the reported that twenty nine states had signed (but not ratified) the convention.

The International Labour Organization (ILO) is a tripartite UN agency which states as its mission as bringing “decent work and livelihoods, job-related security and better living standards to the people of both poor and rich countries...by promoting rights at

work, encouraging opportunities for decent employment, enhancing social protection” In its Convention 182, the ILO demands the prohibition of the worst forms of child labour which includes the “production of pornography or for pornographic performances” (ILO). Canada ratified the ILO Convention on the Elimination of the Worst Forms of Child Labour which led in part to the UN (2003) praising Canada’s efforts and initiatives (Library of Congress: 2007, 59). Laws regarding “child pornography” exist in Canada, and include sentencing guidelines for convicted offenders. The range of offences refer to the printing, publishing, transmission, and distribution of pornographic materials, and to the luring a child. Importantly, as “child pornography” has been identified as “intra-family” violence, with the majority of children suffering abuse within their families (Herschel: 2003, 9) Canada also has laws against householders who permit illegal sexual activity and corrupting children (Library of Congress: 2007, 57).

The (UN) Optional Protocol on the Sale of Children, Child Prostitution, and Child Pornography defined child pornography as “any representation of a child engaged in real or simulated explicit sexual activities or of the sexual parts of a child for primarily sexual purposes” and stated that child pornography was “the evidence of the sexual abuse of a child and that the production of child pornography always presupposes a crime committed towards the child” (Sutton, 2004: 5).

Under Article 34 of the Convention the Right of the Child, Canada is legally bound to protect *all children* from all forms of sexual exploitation and abuse (Feres: 2004, 18). In the protection of children overseas (e.g. objects of travel for the purpose of sexual

exploitation, aka “sex tourism”) Canadian law was enhanced by Bill C-27 that extraterritorially extends the Canadian Criminal Code to allow the prosecution of Canadians who commit offences against children overseas (Feres: 2004, ). This is not the case elsewhere as many countries around the globe do not have extraterritorial laws. Where extraterritorial laws do not exist, foreign citizens can presumably commit offences against children while travelling (in Thailand, for example) and not be prosecuted in their home country for crimes committed elsewhere.

Moreover, the possession of images of child abuse is not illegal in some countries, including Russia. The International Centre Missing and Exploited Children actually reported that there are forty-one countries that do not criminalize ‘child pornography’ (Quayle, 2008: 87). Images of real children being sexually assaulted only recently became illegal in Japan. However, to this day, animated, ‘pseudo’ depictions of child rape are part of a huge market in Japan where images of children (appearing as young as primary school) being gang raped by adult men continue to appear in Japanese computer games, and on the front covers of magazines and comic books (Quayle, 2008: 18). Sadly, Japan is not alone on this shameful stage.

One leading international child protection agency, ECPAT, reported that Russia was one of the main producers of child pornography in the world (ECPAT, 2004). At the 2008 World Congress III Against the Sexual Exploitation of Children and Adolescents, attendees reported that many states’ laws still do not adequately define and criminalize the sexual exploitation of children in accordance with application international standards

and fail to recognize the special status of child victims (Rio World Congress III Outcome Document: 2008, 3). Possession and production however do not address the sordid practice of 'viewing' in absence of downloading or saving images. Quayle (2008) reported at the III World Congress that not all legal instruments define the intention viewing of Internet 'child pornography' as criminal (Quayle, 2008: 3). Quayle remarked that it was surprising to find that international instruments did not criminalize viewing; she quoted Gillespie's (2008) conclusion that the UN Protocol does not mention 'viewing' and that the Council of Europe refers to it 'obliquely'(Quayle, 2008: 3). In the context of an international phenomenon inconsistent definitions and legal interpretation make the challenges of enforcement much more daunting.

Canadian law includes a broad definition of 'child pornography' that covers all the acts defined in the Optional Protocol. The laws that address child pornography on the Internet are entrenched in the Canadian Criminal Code, amended by Bill C-15A, which received royal assent in June 2002. This Bill amended the Criminal Code by creating new offences and enforcement measures to deal with sexual exploitation, particularly as it related to the Internet. The Bill also created the offence of accessing child pornography. Specifically, the Canadian Criminal Code made it an offence to possess any child pornography, and to make, print, publish, or possess, for the purpose of publication, any child pornography. It is illegal to import, distribute, sell, or possess, for the purpose of distribution or sale, any child pornography (section 163.1; 163.2; 163.4).

In 2002, Section 172.1 was added to the Canadian Criminal Code criminalizing electronic communication with a person, believed to be a child, for the purpose of facilitating the commission of sexual offences, generally referred to as 'child luring' (Criminal Code R.S., 1985, c. C-46). Since these amendments were made, it is an offence to transmit and make child pornography available by posting it on a website or offering information on where to find child pornography on-line. Finally, the Bill enhanced judicial powers by allowing judges to order the deletion of child pornography posted on computer systems in Canada.

Effective Canadian legislation is not yet in place and contains several loopholes (ECPAT, 2006). Gaps in legislation include the fact that in Canada mandatory reporting of suspicious material is not required of internet service providers (ISP) in eight of ten provinces in Canada (NOVOC, 2008). As the results of this study documented, in Canada, cooperation of ISPs in police investigations is only guaranteed by judicial order. Thus, the exchange of illegal or suspicious materials is not automatically referred to the police, and when illegal materials are identified by police or cybercrime hotlines, the ISP is not required to render the customer name and address to the police without a search warrant or production order.

Notably, in a February 2009 Ontario Superior Court Justice Lynne Leitch, in a possession of child pornography case, found that there is "no reasonable expectation of privacy" in subscriber information kept by Internet service providers" (National Post). This ruling, which binds lower courts in only Ontario, represents the first time a Judge in

Canada has ruled on whether there are privacy rights in ISP information that are protected by the Canadian Charter of Rights and Freedoms. This ruling heralds a significant move forward for child protection advocates and police investigators.

### **Pervasiveness of the Crime and the Role of the Internet**

It has been reported that the sexual exploitation and sexual abuse of children has grown to worrying proportions at both national and international levels, in particular in regards to the increased use by both children and perpetrators of information and communication technologies (ICTs), and that preventing and combating such sexual exploitation and sexual abuse of children requires international cooperation (CDPC, 2007: 2-3). Further, it has been suggested that approximately five million images of child abuse are in circulation on the Internet featuring some 400,000 children (ICE, 2009). In May 2009, 125,000 images and videos were located on the computers of a paedophile network operating in the United Kingdom, with images of children as young as three months old (The Times, 2009: 3). The exchange of images of children being sexually abused continues to proliferate and in some instances have become even more extreme (ISPAI, 2008). The Internet Watch Foundation (IWF) claimed that the children in the images they deal with are suffering some of the cruelest forms of sexual abuse, and that these children increasingly appear to be younger. IWF reported a continuing trend in the severity of the abuse in images on the websites our analysts examined and claimed that the illegal use of the Internet by paedophiles continues to be a huge challenge (IWF, 2007: 8).

According to Jenkins (2001), child pornography has a substantial, murky history with many individuals able to find child pornographic materials by resorting to creative subterfuges and new technologies. He claimed that the Internet merely marks the latest phase in this story. It is true that although child pornography existed long before computers and the Internet came into existence, it is also true that the Internet is now a principal medium for distribution. Contact with victims through social networking sites and chat rooms is reported to be growing, and instant messaging was reportedly involved in over half (56 per cent) of child pornography reports to CEOP in the U.K. in 2008 (CEOP, 2008).

The production and ready availability of child pornography in specific parts of the world is troubling. The popular Russian web search system Jandex yielded no less than 405 sites and 19,864 pages in reply to the request for child pornography in Moscow (ECPAT, 2004). Equally shocking, CEOP recently reported the appearance of images containing victims from atypical racial groups and in atypical locations, including South America and Asian countries such as South Korea, China, and Japan. They believe this reflects the role of the internet in facilitating global communications...across language and cultural borders which may not have happened otherwise (CEOP, 2008: 19).

The IWF reported that “during 2006, 10,656 URLs of individual web pages or websites were confirmed by our hotline team to have child sexual abuse content; during 2007, the IWF processed 34,871 reports which resulted in 2,755 top level domains with child sexual abuse content being assessed, confirmed as potentially illegal, traced, and

the appropriate intelligence being disseminated accordingly” (IWF, 2007: 6-8). This level of activity is not uncommon in Canada. Cybertip.ca reported “that since the National Tip line went national in January 2005, over 24,000 reports have been received, and 90% of the forwarded reports are in one of four areas; child pornography, online luring, child sex tourism, and children exploited through prostitution” (CAPB, 2008: 12). In fact, between September 2002 and March 2009, 30,000 reports had been received. Of images reviewed by Cybertip.ca investigators, nearly 40 percent depict the sexual assault of a child by an adult or another child, and nearly sixty percent were under the age of eight – absolutely determined to be prepubescent– and nearly ten per cent babies or toddlers (Cybertip.ca, 2009: 25-35). Notably, reports to Cybertip.ca are voluntary and normally made after the accidental discovery of images of child abuse; the worst imagery – the most severe, rated 6-10 by the Cybertip.ca typography<sup>1</sup> for example – may be passed abuser to abuser via peer-to-peer (P2P) transfer of encrypted files. P2P users store videos and images on their personal computers, and others get access to it through specialized software (Cybertip.ca, 2009: 29).

In the commercial exchange of materials, more recent Canadian evidence suggested that the child pornography industry was conservatively estimated at a value of two to three billion dollars (NCCEC, 2005). In 2008, the Canadian National Child Exploitation Coordination Centre (NCECC) reported that child pornography was a very big

---

<sup>1</sup> 1: indicative; 2: nudist; 3: erotica; 4: posing; 5: erotic posing 6: explicit posing (genital/anal) ; 7: explicit sexual activity; 8: assault involving adult;9: gross assault penetrative;10. sadistic/bestiality (cybertip.ca,2009: 29).

business (CAPB, 2008). “It has been estimated that child pornography on the Internet is an industry worth approximately \$20 billion a year” (Darlington, 2007: 2). In an environmental scan produced three years ago, the NCECC stated that the profits generated through Internet based pornography exceeded 2.5 billion dollars per year, with 72 million Internet users viewing Internet based pornography each year.

The growth of the Internet and its ubiquity provides a much wider exposure to not only legal pornographic sites, but also illegal material. “Daily requests for child pornography performed on the Gneutella search engine totaled 116,000...an excess of 20,000 [new] child pornographic images are posted on the Internet each week” (NCECC, 2005: 8).

According to Wall (2005), there are transformational effects as a result of the Internet which allow for new ways to engage in illegal behaviors. Wall stated these impacts “change the traditional relationships among offenders, victims, and the state by potentially creating entirely new opportunities ...by widening offenders’ reach of opportunity globally, enabling offenders to engage victims in new ways, and providing new means for the organization of criminal behaviors” (Pattavina, 2005: 81). Moreover, crimes are facilitated by the apparent anonymity offered by the Internet. The Canadian Victim of Crime Advocate has recently warned that the threat of child pornography through the Internet poses cannot be underestimated. He reported that the Internet provides an unregulated, instant word-wide distribution network that is immediately accessible for viewing, downloading, and even wider distribution (OFOVC, 2009: 4).

## **Offenders' Use of the Internet**

As claimed by Sanderson it is not uncommon for paedophiles to target children from other countries in the hope of avoiding detection and/or prosecution, due to different legislation in other countries (2004: 270). According to another authority, paedophiles are highly ingenious in attempting to avoid detection. [The police] still know too little about the criminological aspects of, such as how paedophile rings work in cyberspace and how these rings are intertwined with social networks in the 'real world' (Stol, 2002: 52).

Still, the ways in which sexual offenders exploit the Internet has been studied. Durkin, for example, argued that there were four key criminal acts that sex offenders utilized the internet for: (1) trafficking child pornography; (2) locating children for the purpose of sexual abuse; (3) engaging in inappropriate sexual communications with children; and (4) communicating with other like-minded individuals (Middleton, Elliott, Mandeville-Norden, & Beech, 2006). The on-line community is without borders. Offenders can meet under the guise of anonymity and pretence. Given this, other writers have explored how perceived anonymity offered new avenues for criminal acts. McNulty stated that cyberspace allowed for a previously unavailable degree of anonymity, and suggested that sexual offenders have flocked to on-line communities to share images of child abuse and to discuss their behavior (McNulty: 2007). In 2000, a treatment study of offenders convicted of child-pornography related crime revealed that 85 per cent

admitted to contact offences, and a US Postal Inspection Study provided evidence that 80 per cent of collectors of images were also 'active' abusers (Cybertip.ca, 2009: 17).

A recent investigation in Scotland revealed a web of people who had a common interest in child sexual abuse. They made initial contact via the Internet and used it to share images of child abuse, and discuss the ways in which to abuse children (The Times, 2009: 5). Canadian researchers claimed that more than half of child pornography offenders either abuse or attempt to abuse children, and research conducted at Toronto's Centre for Addiction and Mental Health indicated that "the offenders who were convicted of the possession offences had a higher chance of exhibiting a paedophile attraction to children than men who actually molested children" (Centre for Addiction and Mental Health, 2009). Dr. Michael Seto concluded that child pornography offending was a valid diagnostic indicator of pedophilia (Centre for Addiction and Mental Health, 2009).

Some researchers in the field of adult offending, particularly sexual offences against children, have claimed a link between technology and the crimes that paedophiles commit. Quayle and Taylor, who studied the use of technology and their use by paedophiles, concluded that computers act as an aid for those who are sexually interested in children and allow for the production, viewing, storage, and distribution of child pornography. The Internet also allows paedophiles to communicate with each other and act as a conduit for contact with potential victims (2003: 331). Graham Hill, Head of Behavioural Analysis at CEOP (2009), argued that there was a spiral of offender

behaviour, with sexual perceptions and interests at one end and contact offences at the other; however, the motivation was always a sexual interest in children (CEOP, 2009, Conference Notes).

Quayle and Taylor (2003) found that the collection and exchange of images of sexual abuse served to normalize the activity for offenders. The offenders distanced themselves from personal responsibility in the act of sexual abuse. They reported that some of the paedophiles used images as a stimulant and plan for contact offences (Quayle and Taylor, 2001: 365). "Some are sexually attracted to children, others collect extreme pornography of many varieties, and others are off-line molesters who upload images of the abuse to the Internet" (Berkman Centre for Internet and Safety, 2008: 97). Another writer, Schell, argued that at least 80% of those who purchase child pornography are contact offenders and child molesters. He claimed that "police estimate that over 50,000 children worldwide are abused and used as child porn actors", and that "pornography is progressive, besides being addictive... it is no surprise that child porn is becoming so vile and so prevalent on the Internet" (Schell, 2007: 47).

Notably, other researchers, including Lanning (1992), claimed that paedophiles almost always collected child pornography, while Taylor and Quayle warned that in the context of the Internet, it appears that there may be offenders whose activity is limited to viewing and sharing material rather than sexual engagement with children, nonetheless, the uses do include sexual arousal and gratification, lowering of children's inhibitions by exposing them to pictures of other children apparently enjoying sexual activities (Taylor

and Quayle, 2003: 158). The World Congress III Outcome Document, resulting from 2008 Congress III Against the Sexual Exploitation of Children and Adolescents called for the establishment of mechanisms and programs to address sexual offender behaviour, including recidivism through risk assessment and offender rehabilitation and management programs (Rio de Janeiro Declaration and Call for Action, 2008: 9).

### **Victimization and Nomenclature**

The Office of the Federal Ombudsman for Victims of Crime (OFOVC) rightly stated that children cannot consent to sexual relations. For this reason, use of the term 'child pornography' mischaracterizes sexual representations where children are involved. The term does not properly convey the very real harm that is experienced by young victims and the seriousness of the activities of those persons who sexually exploit children in this way (OFOVC, 2009: 14). Indeed, 'child pornography' is more accurately described as images of child abuse or visual/digital evidence of the sexual assault of a child. In the 2009 analysis of website images, Cybertip.ca identified that nearly forty per cent of images depicted sexual assaults against children, which have been differentiated from exploitive child modelling, sexual posting, and genital nudity. These images include the anal and vaginal rape of children by adults (Cybertip.ca, 2009; 34).

Regrettably, the term 'child pornography' is entrenched in key pieces of Canadian legislation and the international lexicon. Quayle (2008) stated that the term 'child pornography' was much more than semantics, and that its use in international policy and law was problematic in its implication. She argued strenuously for the use of terms such

as 'child abuse images' in part to establish some valid quantitative measure of the problem (Quayle, 2008: 82). Researchers have argued against the use of the terms 'child pornography' because that simply implies conventional pornography, but with child 'subjects'. As such, it is an inappropriate term to describe recorded images of the sexual abuse of children. Some researchers have taken the position that photographs of child sexual abuse are photographs of a crime in progress (Silverman and Wilson, 2002: 90) and, by definition; no child can give consent for their involvement.

Recently, Newell (2008), in his presentation at the III World Congress suggested that, rather than using the terms 'child pornography' that the terms 'sexual exploitation of children in pornography' and 'representation of sexual abuse' be utilized (Newell: 2008, 8). Authors of the 2005 National Juvenile Online Victimization (N-JOV) Study stated that they used the term 'child pornography' only because it had been used in American court decisions and statutes, and was readily recognized by the public. When the euphemistic term 'child pornography' is used in this major paper, it is intended to reflect the image of child sexual abuse and the pictorial evidence of a serious criminal act.

Hodgson and Quayle (2003) quite properly argued that child sexual abuse images required that a child be abused to produce it, and that the production required the photographer to create a situation where a child was abused. They also correctly claimed that "child pornography can act as a learning instrument in the 'grooming' process, whereby a child is de-sensitized to sexual demands and encouraged to normalize inappropriate activities" (Hodgson and Quayle, 2003: 26). Other researchers agreed that

photographs of children engaged in sexual activity might act as learning tools in the grooming process or be employed to entice other children into the same behavior with devastating consequences (Sheldon and Howitt, 2007).

The effects of the crime of child pornography are as devastating as they are pervasive. Child pornography objectifies and degrades its victims, is used by abusers to manipulate children, and allows the offender an opportunity to minimize his involvement in a crime (Sutton, 2004). Some academics claimed that the offence was serial in nature. For example, Davidson (2007) stated that a child was victimized every time their image was Retrieved and viewed, and that images [or videos] on the Internet potentially formed a permanent record of abuse. Harrison (2006) claimed that knowing that this permanent video or pictorial record existed exacerbated the child's trauma and the feelings of powerlessness and shame they experienced.

Health Canada stated that 'sexual abuse' referred to the use of a child for the sexual gratification of an older adolescent or adult and involved the exposure of a child to sexual contact, activity, or behavior, including exploitation, such as pornography (Health Canada, 2002). Whilst the psychological impact of sexual abuse on an individual may be incalculable, Health Canada has identified over a dozen observable effects as consequences of child abuse, including extreme and repetitive nightmares, anxiety, unusually high levels of anger and aggression, and feelings of guilt and shame. Of particular concern for sexual abuse victims, feelings of guilt and shame can be quite

severe, especially if the victim experienced some degree of pleasure during the criminal act (Health Canada, 2002).

### **Challenges in Policing the Crime**

The existence of child pornography on the Internet presents law enforcement with diverse, complex challenges. Wall (2005) stated that Internet or cybercrimes are free of a physical time frame, are transnational, trans-jurisdictional, and global. He cited the lack of consistent reliable statistics as a hindrance to studying cybercrime, and, by extension, the tracking of Internet based child exploitation crimes. He stated that victimization questionnaires (absent in some many parts of the world) were “the only way in which reliable statistics about individual victimization can really be captured” (Wall: 2005, 86-87). The Canadian Centre for Justice Statistics (CCJS) reported that there were no national data regarding cybercrime, a branch to which child pornography on the Internet most certainly belongs.

The extent of child pornography on the Internet has not been consistently tracked and reliable statistics are simply not available. Surprisingly, Canada presently does not have a uniform method of collecting data on cybercrime activity (CCJS, 2002). NCECC stated that “there is little empirical data on the breakdown of the child pornography industry in Canada...while assumptions can (and often are) made, it is important to develop research energies to these areas” (NECEE, 2005: 8). Taylor and Quayle (2003) also identified a lack of research or data collection in this area by stating that there was very little empirical data about child pornography.

Given the state of official statistics on the amount of internet-based child pornography, it was not surprising that studies on police effectiveness in this area were very rare. According to Rogers et al., “there is a lack of studies that examine how law enforcement agencies are dealing with digital evidence and that, while the vast majority (80.0 per cent) of all cases involve digital evidence, the quantity may simply be overwhelming the police” (2007: 42). Indeed, other researchers, such as Holland (2005), concluded that, despite policing efforts, few children were ever identified from Internet-mediated child pornography pictures. Others have argued that “the lack of skilled and knowledgeable officers in cybercrime seriously inhibits their success rate” (Hodgson and Orban, 2001: 64).

Wall (2007) summarized the challenges facing police as: obtaining funding; jurisdictional obstacles; the ‘routinized’ practices of traditional policing; and the inadequacy of criminal procedures to deal effectively with inter-jurisdictional cases. Prior to this, Stol (2002) claimed that the challenges were: a lack of knowledge; barriers in collaboration; and obstacles in criminal investigation. Stol went further by arguing that all officers needed specific knowledge and training regarding digital equipment, as well as local expertise in securing digital evidence. Moreover, at the local and national level, officers required expert specialization (Stol, 2002). Attendees at II World Congress Against the Sexual Exploitation of Children and Adolescents called for an increase in training for professionals involved in prevention and protection of children (Rio World Congress III

Outcome Document). However, these recommendations, for the most part, have not been undertaken by police departments throughout the world.

In summary, a broad spectrum of researchers has identified the challenges of policing the crime of child pornography on the Internet. The main challenges identified were: a global legal landscape and lack of legal harmonization across states; the failure of any consistent interoperability between nation states; the immensity and enormity of the problem; the lack of insight into offender behavior; policing practice; and a paucity of reliable data. Given this, this major paper examined these challenges within the framework of existing laws and legislation, the profiles of the offenders, an understanding of the victims, and the efforts of both public and private organizations. Moreover, this major paper reports on the findings of a survey questionnaire conducted across Canada which examined the challenges associated to this phenomenon from the perspective of police officers. This paper concludes with a number of recommendations informed by an extensive literature review and the aforementioned study.

## Chapter One: Literature Review

This chapter provides a comprehensive literature review on the crime of child pornography on the Internet. Specifically, it introduces the main challenges that police face in their attempts to address the crime of child pornography on the Internet. This chapter identifies five key challenges and analyzes how each challenge affects the ability of the police to respond. This discussion is followed by a description of the Canadian police's current response to child pornography on the Internet and places their efforts within the global context.

Awareness of the challenge of policing crimes facilitated by high technology and the Internet has been growing for over a decade. Some authors, including Correria and Bowling (1999), pointed to these issues ten years ago when their research indicated that law enforcement agencies were not adequately prepared for computer-related crime investigations or that the police had not yet developed specialized units to respond to this crime type. Their work, along with the work of others, identified the following five key thematic issues. Combined, these issues make the policing of child pornography on the Internet extremely difficult:

1. Police (locally, nationally, and globally) lacked specific expertise and training;
2. Insufficient empirical data on cyber-based crimes;
3. Police prioritization and budget constraints affected the police's capacity to respond;
4. Policing child pornography on the Internet was affected by the fact that Canadian law did not legislate the reporting of suspicious materials by Internet Service Providers (ISPs); and
5. Cooperative partnerships with governments, non-government organizations, and the private sector needed to be strengthened globally.

## **Expertise, Technology, and Training**

Walker, Brock, and Stuart (2006) referred to 'cyber policing' as 'faceless-oriented policing' and claimed that traditional policing was not adequate in a cyber-world. They argued that "with Internet crime, visible venues of crimes are significantly reduced while invisible venues have expanded exponentially. With a diminished possibility of detection and prosecution, faceless crime offenders with the means (Internet and working computer) will gravitate towards the faceless variety of offending. Cyber investigators are a new entity in the policing world. There are very few capable investigators...too few" (Walker, Brock, & Stuart, 2006: 171-172).

Walker, Brock, and Stuart, along with Healy, and Jewkes and Andrews, all believed that technical knowledge and expertise gaps, particularly as they related to investigating child pornography on the Internet, was a major challenge. The "regulation of child pornography in the computer age presents special challenges that require considerable technical expertise: law enforcement officials around the world require technical training...and governments must be willing to allocate funds for such training and the necessary equipment" (Healy, 2003: 14). The difficulties faced by police officers working within geographical boundaries were infinitely magnified in the borderless world of cyberspace (Jewkes and Andrews, 2005).

According to Wall (2007), the presence of current, relevant specialist knowledge and expertise within a police force determined the degree to which an organizational and occupational response to cybercrime would be effective. Given this position, it was

troubling to discover that most police agencies did not have their own distinct and easily identifiable cybercrime unit or the in-house expertise to respond to cyber-based crimes. Moreover, even within agencies that had cybercrime expertise, the officers may not have the specialist skills or the training necessary to investigate the production, distribution, and consumption of child pornography (Jewkes and Andrews, 2005).

The American Bar Association stated that operational challenges were caused by a lack of equipment, training, and adequate organizational structure locally, and that the need to work with great speed, despite time zone, language, and cultural differences, contributed to the failure of local law enforcement to successfully address crimes globally (ABA, 2003: xxv). Malinowski agreed that “the dilemma that exists is investigators who are traditionally trained in investigations may not have basic computer skills...while a cyber investigation may possess the skills to elicit and develop information from cyber sources, technology issues must be thoroughly understood. Technicians need to be trained for forensic data recovery, documentation, and digital situational awareness” (Malinowski, 2006: 312-317).

Training for law enforcement needs to address the evidential content related to the images with an emphasis on tracking the chain of distribution and viewing the content with a forensic mindset. Mittal, for example, reiterated the importance of child protection and victim rescue claiming that “despite the temptation of putting resources into the detection of the relatively easier offences of possession and trading, the

emphasis must also be on child protection and the identification of children” (2004: 298).

However, according to Ferraro and Russell:

Police officers cannot keep pace with the evolution of technology. There is a great need for forensic scientists to develop tools and tactics to retrieve and preserve evidence from emerging and complex technologies...we need scientists to pioneer methods of extracting evidence and ensuring its stability and integrity. A lack of computer savvy is a serious problem for the police, and is compounded by insufficient training on either computer usage of computer crime...poor training programs may emanate from the occupational culture of the police as well as from fiscal restraints (2004: 9).

Furthermore, Jewkes and Andrews (2005) argued that if police were to be considered competent in combating cybercrime, they must become a technologically literate force of cyber cops.

The European Committee on Crime Problems (CDPC) has long recognized the need for training to carry out investigations with an aim of enhancing professional competence (CDPC, 2007). Europol (2006) in its Analytical Work File (AWF) identified the need to train law enforcement officers to investigate child abuse on the Internet according to global law enforcement standards (Europol, 2006). The European Information Society (EURIM) demanded that the Skills for Justice, the national centre in the United Kingdom responsible for ensuring adequate training and skills strategies, address the capacity gaps in Britain.

Notwithstanding the research conducted within Canada, the dearth of police expertise and the availability of training were consistently identified as lacking elsewhere. According to McAfee (2008), law enforcement remained ad hoc and ill-equipped to cope with the demands of responding to and preventing cybercrimes. He suggested that there was a significant lack of training and understanding in digital forensics and evidence

collection not only by police, but by the law courts nationally and internationally. While the “technical training for law enforcement in Canada is regarded as one of the highest caliber available...situations exist where designated technological crime investigators had to wait over a year to attend their first foundational Canadian Police College training course in the investigation of technological crime” (CAPB, 2008: 11). Providing police officers with intensive two or three week courses to learn about the Internet is simply insufficient.

### **A Paucity of Data**

A second challenge identified in the research was that accurate data on the actual level of cybercrime and child pornography on the Internet does not exist. Henschel (2003) pointed to the specific problem of data shortage, and linked the problem to poor data collection methods particularly related to investigations and prosecutions in cases of the exploitation of children. While many of the problems associated with policing child pornography on the Internet have been known for over a decade, little empirical study and statistical tracking has occurred. No reliable longitudinal studies have been conducted, and cybercrime data regarding child pornography facilitated by the Internet, exchanged via cell phones, or viewed on I-phones are almost non-existent.

Attendees at the III World Congress Against the Sexual Exploitation of Children and Adolescents also claimed there continues to be a lack of reliable data on both the prevalence and the nature of sexual exploitation of children (Rio de Janeiro Declaration

and Call for Action, 2008: 4), while Muir (2005) stated that there is an overwhelming lack of information and research combined with [public and private] accountability and responsibility, and he reminds us of legislative gaps, inconsistent laws, and different definitions that give rise to policing challenges. Other researchers have argued that “law enforcement, specifically on the municipal level, is not prepared to effectively handle computer-related crime, nor, for the most part, is it preparing for such crime” (Correia and Bowling, 1999: 240). Smith recommended that “official statistical data collection should seek to explore more useful categorization of cybercrime when collecting data from police, courts, and corrections agencies ...at present, conventional crime statistics simply do not enable any differentiation between cybercrimes and other types of evidence” (2004: 155). The absence of reliable data makes decisions regarding local police resource planning and expenditure much more difficult. This challenge is compounded by crimes that occur in the international ‘virtual’ world, rather than in the local ‘real’ community with which police officers are more familiar.

The Canadian Justice Centre has also researched this phenomenon and reported that “a range of factors, including the absence of an uniform definition among police departments, the lack of formal policies and procedures within specialized units, and the lack of resources provided to specialized unit investigating Internet or computer crime contribute to the challenges in collecting accurate statistics” (2002: 26). Correia and Bowling noted that “although it has been suggested that law enforcement is not prepared

to address computer related crime, empirical data scarcely exists to verify or nullify such a claim” (1999: 228).

Despite the paucity of existing research specific to Internet based sexual offences in Canada for some time, more recent work has given voice to the increasing public and police concern. The publication “Every Child, Every Image” released in May 2009 stated that “more than 90 per cent of Canadians are concerned about the distribution of child sexual abuse images, and child sexual exploitation is ranked as one of the top three concerns for parents regarding children” (OFOVC, 2009: 2). The authors of this report claimed that “the number of charges for production or distribution of child pornography increased by 900 per cent between 1998 and 2003, and yet, only 33 per cent of those convicted of distribution were sentenced to prison while 52 per cent received probation” (OFOVC, 2009: 2). It is difficult for a criminal justice system to consider a response to any criminological challenge when the breadth of that challenge is unknown. The fact that real data that adequately and accurately reflects the scope of the production, viewing, and distribution of images of child abuse does not exist poses several serious challenges to public policy and decision making, such as police priority setting.

### **Police Priority Setting and Budget Impacts**

In local communities, police priority setting effects law enforcement’s capacity to deal with crimes that occur in cyberspace. Some authors argued that the priority that law enforcement place on specific crimes was related to financial resources and budgeting

processes. However, O'Donnell and Milner concluded that "the potential for cybercrime is so enormous, it could consume a budget of almost any size...police forces must determine how to ration the finances at their disposal based on some objective assessment of the problems they face" (2007: 157).

Wall argued that "local police forces work within tightly prescribed budgetary parameters and often simply cannot cope with demands to investigate the crimes arising from globalized electronic networks" (2007: 210). "Policing, within the global system of criminal justice, needs to adapt its priorities and practices in order to respond to the dynamic nature of criminality" (Russell, 2003: 121). According to Russell, law enforcement was an evolving vocation where police officers must be able to adapt to dynamic conditions. However, with cybercrimes, adaptation required constant investments in upgrading the skills and expertise of officers, the available technology, and the cooperation of stakeholders in the private and public sectors.

The McAfee Security Report (2008) observed that "despite the evident increasing risk to national security, governments are still floundering at the first hurdle when it comes to cybercrime. They are failing to view cyber security as a priority due to technical ignorance and lack of foresight of the widespread and longer term risks and are neglecting to prioritize legislative time and resources to it" (2008: 9). It is clear that competing priorities exist in policing, and that crimes committed by way of technology, including child sexual abuse images on the Internet, do not always rank among the highest priorities for police.

## **Legislative Gaps**

The fourth challenge to effective policing of child pornography on the Internet is that, under Canadian law, the reporting of suspicious materials is not legislated. In Canada, the reporting of illicit materials viewed, exchanged, or Retrieved by an ISP's customer is voluntary. By way of comparison, in Britain, ISPs are legally mandated to report suspected transmissions of images of child abuse. As a result of this legislation, 5,812 reports were processed by Child Exploitation Online Protection in 2007 alone (CEOP, 2008).

British Telecom, one leading ISP in the U.K., uses 'Cleanfeed' which is a system that blocks child pornography sites from its 2.7 million Internet subscribers by filtering out specific domain names supplied by the Internet Watch Foundation. Given its success, it is predicted that the legal requirement of ISPs to report suspected images will soon become an integral policing strategy in the U.S.A (McDougall, 2006). Canada also has 'Cleanfeed Canada' as well as Cybertip.ca, which is the official reporting hotline in the country. Cybertip.ca is a non-government organization funded by contributions made by leading ISP providers, including Telus, Rogers and Bell Canada, as well as the government of Canada and some provincial governments. Cybertip.ca provides a centre point for reporting, and is a member to the International Association of Internet Hotlines (INHOPE.) INHOPE was founded a decade ago, and represents Internet hotlines around the globe, and supports them in responding to reports of illegal content (INHOPE, 2009).

Cybertip.ca, along with being the reporting centre, makes an important contribution to new knowledge in the field, and recently produced a document entitled *Child Sexual Abuse Images: An Analysis of Websites* (Cybertip.ca, 2009). This document contains important analytical detail, including discussion of commercial website, types of images, and the location of 'hosting' websites and how purchases or illegal materials are made. The report makes twelve key recommendations that cover a broad spectrum including children, parents, adults, child welfare professionals, business and the general public, which have influenced the recommendations made in this paper.

In its daily work, cybertip.ca compiles lists of offensive sites; however, websites are only blocked on a voluntary basis (Thompson, 2007). As of February 2009, only eight of the more than 400 ISPs in Canada participated with this program (OFOVC, 2009). As the relevance of Cybertip.ca emerges as a research centre, for example, its importance in advocacy is likely to rise. Its place at the international table will increase with implementation of its key recommendations, such as developing collaboration among the world's hotlines (Cybertip.ca, 2009).

The U.S. House of Representatives identified the need to harmonize its laws with those in the U.K. when they recognized that there are important differences between the approach of U.S. law enforcement and its international counterparts. The United Kingdom employs a 'notice and takedown' approach...ISPs voluntarily agree to block access to URLs identified by the Internet Watch Foundation (IWF) as containing images of child pornography and the U.K. police shut them down (Committee on Energy and Commerce,

2007: 19). This approach has reduced the hosting of website containing images of child abuse to negligible levels (Cybertip.ca, 2009). Legislation for mandated reporting is pending in the United States.

For the savvy computer user, posting materials and creating websites located in countries where legal gaps such as these exist presents little challenge. The legal diversity across nations has created an environment in which child 'pornographers' operate in opportunistic ways. Evidence consistently demonstrates that sex offenders operating on the internet are indeed a savvy group. In developing profiles of suspects, CEOP stated that "IT professionals are comparatively prominent...reflecting the technical capability of some on-line offenders (CEOP, 2008: 18). Offenders need Internet service providers (ISPs) to access the Internet, therefore ISPs are in the best possible position to assist in the fight against images of child abuse on the Internet, despite their contention that the vast amounts of material passing over their servers, render it almost impossible to do so (Hetch, 2008: 10). Canada only recently introduced legislation requiring mandatory reporting. Until this recent announcement, legislation did not address the need for ISP cooperation. The pending legislation contained in Bill C- 46 received first reading in the House of Commons June 19, 2009 but has not yet become law.

## **Cooperation and Capacity across Borders**

One researcher stated that “essential to the successful interdiction of cross-national cybercrime are three factors: legislative harmony; a framework of law enforcement cooperation; and the capacity to investigate and, if necessary, to prosecute (Grabosky, 2007: 14). Others have claimed that the size of the Internet, its traffic volume and diverse legal approaches and inter-jurisdictional difficulties combine, resulting in the police feeling that they are constantly trying to ‘catch up’ (Jewkes and Andrews, 2005: 50). It is heartening to discover the recent studies conducted by the Canadian Association of Board of Police and the Federal Office of Victims of Crime, as well as pending legislative changes in Canada that demand enhanced training, cooperation, and legislative harmony. However, the research conducted for this major paper surveyed the perceptions of Canadian officers, and the results documented that some officers believed that they were losing the war on cybercrime.

The challenges discussed in this chapter are not exclusive to Canada, the United States, or the United Kingdom. The International Centre for Missing and Exploited Children (ICMEC) quantified the existence of five criteria across the 187 Interpol-member countries regarding child pornography on the Internet: laws specific to child pornography; definitions of child pornography; the criminalization of computer facilitated offences; the criminalization of possession; and any legal requirement for ISPs to report (ICMEC, 2006). The findings of this study revealed that only five member countries met all of the criteria, while 95 countries, or more than half of Interpol member countries, had no legislation

that specifically addressed child pornography at all (ECPAT, 2006). Forty-three countries, including the United States, signed the Council of Europe's Convention on Cybercrime launched nearly a decade ago in 2001, with the U.S. ratifying the Convention in 2006. To date, Canada has signed, but not ratified the agreement. The Convention's main goal was to establish a 'common criminal policy' to better combat computer-related crimes worldwide through harmonizing national legislation, enhancing law enforcement and judicial capabilities, and improving international cooperation (Congressional Research Services, 2006).

### **The Canadian Response**

In order to respond to child exploitation facilitated by technology, the Canadian police sector integrated municipal, provincial, and federal policing efforts through the creation of the National Child Exploitation Coordination Centre (NCECC). The Centre was launched in 2003 to serve as an information portal for the law enforcement community, but also to advance research, education, and prevention in the area of child exploitation. Its mandate was consistent with the national strategy on child exploitation which emphasized information sharing, the cooperation of partners, and an improved complaint system and legislative tools. G8 countries, including Canada, committed to combating the sexual exploitation of children online through eight broad actions, including: law enforcement tools/training; intelligence and information gathering; dissemination and

sharing; international cooperation; prevention/awareness; industry and non-governmental (NGO) cooperation; victim identification; suspect location; and legislation (Treasury Board, Government of Canada, 2007).

In addition to the NCECC, Integrated Child Exploitation (ICE) units bring together municipal or city police with federal (RCMP) and provincial (e.g. Ontario Provincial Police) officers to work collaboratively. This is a burgeoning model of partnership which could be emulated by other police forces around the world. The units are highly regarded by some, and as Deloitte and Touche reported “as a partnership between federal and municipal law enforcement agencies, the ICE units use dedicated investigators and coordinated efforts focused towards a single objective of investigating child pornography and exploitation matters. Their collaboration and dedicated efforts are leading to higher levels of detection and conviction” (CAPB, 2008: 12). Nonetheless, as research for this major paper documented, not all provinces have ICE units, and respondents to the study questionnaire demanded that this be changed.

The proliferation of child pornography occurs in opportunistic locations, where detection and investigations are less likely to occur. According to ECPAT (2008), more commercial sites dedicated to child pornography have appeared in recent years allowing anyone with a debit or credit card to purchase child porn. The fact remains that there are approximately 2,000 to 3,000 internet domain addresses identified each year worldwide that provide child abuse images (CEOP, 2008). In some European countries, cooperation between hotlines, police, and internet service providers quickly block sites containing

child pornography, immediately disrupting any commercial activity. Still, as this literature review highlighted, a global approach, where organizations and countries harmonize legislation, work cooperatively, and share intelligence, regardless of borders, is required to reduce the opportunity to purchase child pornography on the internet and prevent producers of this material from engaging in this illegal activity.

Important private partnerships do exist, however, and are being championed by leading international corporations such as Microsoft, which has developed a strategy to address crimes facilitated by technology that includes technology, education and awareness, cross-industry, and public private partnerships. The Child Exploitation and Tracking System (CETS) is one example of a technology that was collaboratively developed by Microsoft in consultation with the RCMP and the Toronto Municipal Police, and which now has an international foothold in assisting law enforcement. The program, which can be tailored to local laws and practices, allows investigators (or police officers) to “capture, share, and search information at all levels of an investigation” and saves the intelligence (e.g. images) in a database. This program has resulted in the successful rescue of children in Canada and the U.K. where it is used by CEOP (Microsoft: 2008). Now fully engaged in twenty ‘developed’ countries it is now being piloted for use in developing nations where public policy and child protection practices are not yet aligned with modern technology. The University of Victoria’s International Institute for Child Rights and Development is taking a lead in this CIDA funded project.

And, the work with other academic partners continues. For example, as recently as December 2009, Microsoft announced the launch of a new product entitled, PhoDNA, which was created in partnership with Dartmouth College. PhoDNA, which works with video images as well as still images, is referred to as robust hashing – a forensic identification process that is designed to identify images that have been changed, and prevent the recirculation of old, but altered images (NY Times, 2009).

It is clear that the private sector and the advances being made in technology within this sector, often in cooperation with law enforcement, are key strategies to minimize criminal activity that is facilitated by technology. The continued efforts to make the Internet a safe place to play, learn, and conduct business and commerce are important elements of good business and public policy. While, evidence documenting these efforts is located throughout this paper, the recommendations also call for greater attention and a more formalized relationship, such as industry councils. Research results, as detailed below, indicate the opinions of Canadian police officers on this, and other critical topics.

## **Chapter Two: Methodology and Results**

### **Methodology**

The methodology used to gather data for this major paper was a survey questionnaire (See Appendix) sent to all 224 municipal police forces in Canada and to 70 RCMP detachments in Canada contracted by local governments to provide policing in cities and municipalities across Canada. A database of police forces in Canada was

provided by the Police Sector Council. Consultations about the survey and the study methodology were held with the Chief of Police of the New Westminster Police Service, Lorne Zapotichny, Chair of the Association of BC Chiefs of Police, and with Chief Superintendent, Richard Bent, of the RCMP, OIC of Contract Policing in British Columbia. Letters of support from Chief Zapotichny and Chief Superintendent Bent accompanied the survey and were personally addressed to the Chief of Police at every service and/or detachment. An introductory letter from the author outlining the purpose of the study was also included in the mail out package.

Draft questionnaires to be included in the survey were shared with Dr. Roberta Sinclair, Ph.D. (RCMP), and DCC Stuart Hyde, LLB, Cumbria Police Constabulary, both of whom are published authors whose professional work includes policing, research and education, and working with international partners to eradicate the exploitation of children. All of the comments made were integrated into the final version of the survey. The questionnaire was translated into both Canadian official languages, and French versions were sent to all Quebec-based police services. Return envelopes were coded to differentiate between municipal and RCMP detachments, but no city, service, or personal identifying system was employed that would allow the researcher to identify respondents.

The questionnaire was designed to explore five key capacity themes and to obtain the opinions of police officers who conduct investigations into the crime of child pornography on the Internet. The main themes of the survey were:

1. Perceived officer capacity regarding knowledge, skills, and experience;
2. Opinions regarding the police's expertise in Canada and globally on these issues;
3. Detachment demographics;
4. The existence and composition of specialized units; and
5. Training specifics

The questionnaire included 15 close-ended statements using a four point Likert scale with the response options of: strongly disagree; disagree; agree; and strongly agree. Notably, in order to identify the degree of importance that officers placed on certain issues, the questionnaire asked respondents to rank order the specific areas of technology, finances/resources, and personnel. In order to identify where best practices might exist around the globe, the questionnaire asked that respondents provide an assessment of the expertise of the police in different countries. Finally, respondents were encouraged to provide any additional comments about the capacity of Canadian municipal police forces to respond to child pornography on the Internet. This open-ended question was intended to provide an opportunity for respondents to include any personal concerns, observations, and comments related to the issue of policing child pornography on the internet.

Questionnaire instructions asked that the questionnaire be completed by officers responsible for the investigation of cybercrime. While a preferred return date was specified, a reminder letter was also sent to each recipient three weeks after the initial mail out. Two weeks after the formal deadline passed, the surveys received by the researcher were entered into SPSS, a statistical program designed to analyze quantitative

data. Nearly half of the respondents (42.4 per cent) provided additional comments in the section provided. The essence of these comments has been captured throughout the discussion and recommendations sections of this major paper. Finally, and as an aside with respect to methodology, it should be noted that the research process and methodology used for this paper was approved in advance by the Ethics Review Committee of the University of the Fraser Valley. The certificate is archived with Research and Graduate Studies, UFV.

## **Research Results**

Of the 70 questionnaires sent to RCMP detachments, 49 were completed and returned (70.0 per cent). Of the 224 questionnaires sent to municipal police forces, a total of 73 were returned (32.5 per cent). The response rate for the survey overall was 41.4%. Of the entire sample, a slight majority of respondents (57.9 per cent) were municipal police officers.<sup>2</sup>

As mentioned above, one of the main themes of the survey was to assess the police's capacity to respond to child pornography on the Internet. To begin, just over half of the respondents (56.1 per cent) did not feel that the laws in Canada were adequate to enable police to respond to child pornography on the internet. A large majority of respondents (83.4 per cent) indicated that they did not believe that the police had enough trained personnel. Moreover, nearly three-quarters (70.1 per cent) reported that

---

<sup>2</sup> Tests for statistically significant differences between the RCMP and municipal responses were conducted; none were found to exist in relation to any of the key analyses conducted for this major paper.

the police did not have adequate knowledge of the issues and two-thirds felt that the police did not have the skills necessary to investigate this type of crime. According to one respondent “this type of investigation is beyond the capacity of a detachment. It requires skills the average investigator, in small and medium detachments, does not possess”. A decade ago, following a baseline study of law enforcement ‘preparedness’ specific to cybercrime, Corriea and Bowling claimed that “local law enforcement officers are usually first responders to crimes; hence, their ability to effectively examine and secure computers at crime scenes is of paramount importance” (1999: 230). Remarkably, ten years later, the data from this current study also demonstrated a general lack of preparedness. In some police forces, protocols designed to guide officers in their investigative techniques to ensure that evidence was gathered and secured appropriately had not been standardized or simply did not exist for cybercrime. Some research indicated that difficulties experienced in cybercrime investigations and prosecutions are due to insufficient training to a level of expertise for law enforcement (Security Watch, 2006: 54).

In this current study, approximately half of the respondents (49.2 per cent) reported that standard operating procedures (SOPs), protocols, and guidelines that directed police officers in how to secure digital evidence, such as computer hard drives, had not been initiated in their detachment. More specifically, only one-fourth of respondents felt that the officers with whom they currently served knew exactly what to do with a computer or its peripherals when they were the first responders to a crime

scene in which computers and/or peripheral were present. One respondent commented that “there has been no specific training in cybercrime [and] it is impossible to get on top of this problem”. Another respondent remarked that “we do not presently have enough front line police officers to begin with”.

To determine the police’s level of investigative competencies for child pornography on the Internet, the survey asked respondents about four key skills: email tracking; ISP tracking; covert investigations; and evidence gathering. The responses from participants suggested that much more had to be done to provide police officers responsible for investigating cybercrimes with the skills and knowledge necessary to be successful. For example, according to the survey data, only half of respondents (51.9 per cent) believed that the officers who investigated cyber crime in their community police service had been trained in tracking the source of an email. A similar proportion (52.8 per cent) reported that officers could identify the originating ISP. A much smaller proportion (39.6 per cent) felt that officers had been trained appropriately to conduct covert cybercrime investigations, a crucial skill in conducting on-line undercover operations. However, more than two-thirds (70.5 per cent) reported that officers had been trained in how to gather evidence in relation to investigating child pornography on the Internet. In the section allowing respondents to make additional comments, one respondent stated that “a lack of education by investigating officers, [and] the huge [amount of] time between seizing the computer and having it analyzed exceeded a year [which] is a problem”. Another respondent added that “internet investigations Level 1, 2, 3 has been

provided, but internet investigators are assigned to other duties full time such as general duty". Another respondent said that "the technology does not keep up with the needs of investigators, nor it is affordable to small units".

Not surprisingly, a large proportion of respondents (81.1 per cent) indicated that specific cybercrime training was not provided on a regular basis, and approximately three-quarters (76 per cent) claimed that the training was not current and had not kept up with technology. According to one officer, "I would suggest 90% of members in my office do not have a clue how to investigate these types of crimes". Another commented that "our service has one officer assigned to investigate all matters related to computers including analyzing hard drives. The officer is also responsible for network and other matters and therefore has little time to dedicate to cyber crime matters. I hope this will change in the future". According to another respondent:

To date, there has been no specific training in regard to cybercrime. There are some people who are knowledgeable and we have several people who we contact for direction and advice. The Internet is so wide and large that it is impossible to police. It is hard to know how large the problem is and how it affects the community. In order to get the resources needed for these investigations, you also have to convince the public that the problem is as big as it is. Training, personnel, and technology all costs a lot of money and puts a strain on already cash-strapped municipalities.

Finally, one officer commented "why, if the exploitation of children by child pornography is one of the national priorities of government, has the national police force understaffed their units?" As reported by respondents, a dearth of trained personnel may explain why

investigative backlogs were estimated to be between one to seven months in three-quarters of cases.

Several respondents commented on the amount of time that cybercrime investigations took. For example, one respondent suggested that “forensic examinations take far too long”, while another officer claimed that the “RCMP is required to use tech crime units for all forensic examinations with extremely long wait periods [and] it is one thing to seize a computer under warrant and have the investigation progress. It hits a wall once you have to wait for the examination of the drive.” Another respondent commented that “to enhance investigative excellence, a national unit is required in each province...if properly trained; [it] could provide a uniform basis on to achieve best results. Victim rescue is of vital importance, thus training, funding, and proper manpower levels require substantial increases”.

Throughout the summative comments, Canadian police officers reported that they were not equipped to deal effectively with the pervasive and growing international phenomenon of images of child abuse on the Internet. One officer reported that “municipal police services that look after smaller communities, and only occasional pornography investigations, do not have the expertise, technology, or resources to handle long, complicated investigations”. Another cited officer inexperience, “the majority of front-line officers are ‘new hires’ with experienced officers taken by specialized unit; there is a brain drain underway where there are huge gaps with new hires having not learned the craft of policing, yet managing complex cases”. Still another

respondent stated “any investigation involving multiple jurisdictions always creates logistical and investigational difficulties. With child pornography being distributed almost solely by the Internet, being able to pinpoint these investigations is usually difficult”. Finally, an officer commented that “there are not enough trained RCMP officers to deal with or investigate child porn on the Internet”.

Given these comments, it was not surprising that only one-quarter of respondents (25.6 per cent) indicated that their detachment had a cybercrime unit. Given this finding, it was also not unexpected that less than one-quarter of respondents (23.2 per cent) indicated that there was at least one officer in their detachment dedicated to cybercrime investigations. A similarly small proportion of respondents (25.9 per cent) reported that there was at least one officer in the detachment responsible for investigating “child pornography”. According to one officer, “for the most part, resources are not directed to this type of investigation because there are higher priorities”. Another respondent stated, “Unfortunately, sometimes the attitude among the police is if it’s not happening in my backyard, why should I worry about it?”

Respondents identified that “child pornography” was just one of many crimes facilitated by the Internet, and that cybercrime units were also responsible for investigating a broad range of ‘high tech’ criminal activities. Given this, respondents were asked whether they supported the notion of one centralized, national centre, responsible for officer training, maintenance of databases, and coordination. More than four-fifths of respondents (82.4 per cent) agreed with the idea of a single, centralized Canadian unit. In

fact, nearly half (45.4 per cent) strongly agreed. One officer stated that “the provincial ICE unit is not adequately staffed. These are specialized investigations which require training, equipment, and case law knowledge. Due to current resources in the provincial unit, investigations are being dumped to local detachments without these skills and resources. Thus, cases are not prosecuted after good investigations. Provincial ICE needs to be primary investigator with local support. Right now, it is the opposite”.

When asked about the creation of a single international centre, just over three-quarters of respondents (77.7 per cent) agreed with more than one-third (38.4 per cent) strongly agreeing that this would be a good idea. One officer commented that:

Federal sections in general do not ease the file load of the general duty investigator. I see a greater need for Internet investigators who assist in all types of cybercrimes; porn, fraud, threats, etc... It all requires skills the average investigator, in small and medium detachments, do not possess. The section in [name of place removed for anonymity] is far too stretched for resources and they don't assist in all crimes on the Internet. Skills development far outweighs the need for specialized tech sections that will end up only taking on convoluted, more serious crimes.

The theme of resource shortages was consistent throughout the analysis of the findings from this survey. In fact, a large majority of respondents (83.2 per cent) disagreed with the statement that their police services had the financial or human resources required to effectively investigate child pornography on the Internet.

When asked to rank the three challenges of human resources, technology, and finances, two-thirds of respondents ranked personnel as the leading challenge. This was followed by one-quarter of the sample which ranked finances as the main challenge, while only 13.8% ranked technology as the leading challenge. When considering all of the

rankings, it would appear that the general order was personnel (66.7 per cent ranked this challenge first), technology (46.6 per cent ranked this challenge second), and then finances (47.4 per cent ranked this challenge third). One respondent stated that “given the training and turnaround challenges, a robust support resource is absolutely critical. ICE is our support. They provide good service, but are under resourced”. According to another respondent, “we do the best we can with what we have to work with. My agency is working toward improving its response to CP investigations. However, the move toward improving our ability to respond was not initiated by the leadership of our service. It has been a long battle to receive the training and the resources that I have to date”.

In an effort to ascertain where leadership and best practices might reside, respondents were asked to rank order the capacity of different countries or regions to respond to child pornography on the Internet. It was not unexpected that the United Kingdom would be ranked first by the largest proportion of respondents as a general expertise in policing cybercrime in the United Kingdom has been affirmed by academics, private sector ISPs, Canadian police officers, and non-governmental organizations. Notably, in the United Kingdom, the police operate within a more effective legislative and policy framework wherein ISPs report to the police and the police shut down suspicious sites. Progress is also publically reported. Internet Watch Foundation stated that the percentage of websites hosted in the U.K. dropped from nearly twenty per cent to under two per cent in the course of a decade (ECPAT U.K., 2006: 33-43).

As mentioned above, the research findings reflected the perceptions and opinions of police officers whose work included the investigation of images of child pornography on the Internet. In the main, regardless of where the officers worked, in small or large communities, or whether they worked for the RCMP or a municipal police force, respondents generally voiced similar concerns. In the specific capacities of knowledge, skills, and financial resources, a clear majority of officers (71.1 per cent, 65.3 per cent, and 81.8 per cent, respectively) stated that they did not believe that adequate levels of capacity existed. Alarming, nearly all respondents (98 per cent) also reported that cybercrime training was not provided on a regular basis, and that 'first responders' did not know how to preserve evidence, or even locate evidence, at a scene.

The frustration that officers experienced in dealing with ISPs was perhaps best reflected in the fact that just over three-quarters (76.1 per cent of respondents) did not describe the internet service providers as cooperative without judicial authority (e.g. search warrant or production order). In a dramatic example, NOVOC (2008) reported that an officer investigating live sexual abuse of a child on-line in real time was told by the ISP to get judicial authorization, and only became cooperative when the officer held the phone to the computer speakers, and the ISP provider could hear the child screaming (NOVOC: 2008, 16). This example implies that a cognitive disconnect can occur between the viewer comprehending the authenticity of a contact offence, while perceiving images of it occurring as somehow unreal. It seems that the mediation of the abuse by

technology can serve to diminish its impact. Thus, it is increasingly important to reiterate the reality of the physical acts, and see real children and real victims.

The opinions and perceptions presented are from officers who are regularly engaged in combating the crime of child sexual abuse images on the Internet. Overall, the findings point to a series of barriers and challenges that, if overcome, would result in fewer victims, and the arrest and detention of more offenders. Importantly, the recommendations presented in the next chapter reflect these officers' concerns and represent a call to action.

## **Chapter Three: Recommendations to Improve Canada's Capacity to Respond to the Crime of Child Pornography on the Internet**

In his opening remarks to the conference "Advancing Effective Criminal Justice Response Strategies for IT Enabled Child Sexual Exploitation" held in June 2009, Steven Chabot of the Canadian Association of Chiefs of Police said offenders were separated by geography but connected by the crimes they commit. He stated that while improvements were occurring in justice systems around the globe, there were no indications that child pornography was slowing down, and that police had inadequate resources and that there were serious operational challenges, including investigation and prosecution (CACCP Conference, June 2009).

Based on a review of literature and the findings from this current study, it can be argued that police departments in Canada do not presently have the capacity to effectively respond to the crime of child pornography on the Internet. Perhaps the main limitation is in resources, including personnel. In addition, in many cases, the technology available to the police, particularly at the local level, can be antiquated. As responses to the survey made clear, there are insufficient numbers of trained officers working in too few units. Officers are over-taxed, and cybercrime units, where they exist, are understaffed. Moreover, in general, officers are not adequately trained in the required skills, including email tracing and ISP tracking.

Police officer stress is a topic that has given rise to number of studies that describe the personal and physical toll associated with police work (e.g. Plecas and Anderson, 2002

and Wolak and Mitchell, 2009). It is important, therefore, to keep in mind that police work on specific forms of cybercrimes can be emotionally and mentally taxing. Canadian police officers who must view some of the most disturbing photographs and videos do not receive regular counseling. As one respondent stated, “frustrations in officers [are] due to the lack of support with respect to ensuring the mental health of officers”. One officer reported that sexual health issues developed during the course of his work, and said the problems were compounded by a police culture that does not foster or encourage discussing personal emotional or psychological difficulties that an officer might have related to their police work.

While exploration of this issue is well beyond the scope of the current study, the long-term psychological, emotional, and social effects of working on child pornography cases on police officers demands further research. Wolak and Mitchell have been pursuing this line of enquiry, and recently reported that officers involved in investigations that required them to view images of child sexual abuse present worrying degrees of stress and “personal, family and marital problems” (2009: 3). Many of the officers surveyed in their study reported “sexual side effects – avoidance, intrusive images...overall increased agitation and distress” (2009: 3) They concluded that the exposure to vivid images of child sexual abuse is distinct from other sources of stress in police work, and make a series of recommendations for the well being of police officers struck with these tasks (Wolak & Mitchell, 2009: 3- 11).

In terms of capacity, the gaps acknowledged by Canadian officers are aligned with those identified in the research literature. Indeed, child pornography on the Internet is so pervasive and the investigations are so complex that one country or region alone cannot hope to tackle the challenges of child exploitation facilitated by technology. The research results from this current study highlighted that the capacity of the Canadian police to deal with child pornography on the Internet was failing to meet Canada's national objectives reached in agreement with international partners.

The statements made by survey respondents expressed the efforts made to grapple with cybercrime generally, and their frustration in dealing with child exploitation more specifically. Notwithstanding the national objective to address child exploitation images on the Internet through legislation and policy, the response by Canadian police remains curtailed by its lack of capacity. As highlighted throughout this major paper, success in this area (i.e. rescuing children at risk or locating and arresting offenders) is constrained by finances, priorities, and personnel, and exacerbated by legislative barriers that seriously impair investigations.

Save the Children (2005) called for continuing formal and informal methods of cooperation through Interpol and Europol and demanded that child protection take a more preeminent place in international law enforcement. They argued for a more formalized working relationship, training on international conventions, and a re-definition of "child pornography" and child eroticism, and demanded more active outreach in "sex

tourism” by all nations who have extra territorial laws on the books but are lazier-faire in enforcement efforts (Save the Children, 2005: 12-13).

Research conducted for this major paper also exposed the perception of serious capacity gaps among those responsible for responding to cybercrimes that must be addressed for positive changes to occur. Given the existing research literature and the results of this current study, there are five broad categories of recommendations made to better prevent and respond to the crime of child pornography on the internet:

1. Implementation and enforcement of International agreements, cooperation and assistance;
2. National and international centralized, synchronized interoperable systems at the international level;
3. Local, national, and international private-public partnerships;
4. Canada specific mandated IPS reporting legislation; and
5. Local, national, and international level police training.

### **1. Implementing and Enforcing International Agreements, Cooperation and Assistance**

Grabosky referred to the nature of cybercrime as ‘borderless’, typified by increased sophistication, commercialization, and a sequencing of crimes that maximize profitability (2007: 11). Another author argued that there is inconsistency in international law and demanded that the U.S. use its place of power in the international community to impress on other nations that the eradication of Internet child pornography will happen only if all nations condemn it. Graham (2007) posited that the ‘harmonization of law’ would leave child pornographers nowhere to hide (Graham, 2000: 27).

The G8 called for eight specific objectives, all of which were integrated into the mandate of the Canadian National Child Exploitation Coordination Centre (NCECC). These

included: victim identification; suspect location; international cooperation; law enforcement tools and training; awareness and prevention; intelligence/information gathering; non-government/industry cooperation; and legislation (RCMP, 2007).

However, in the current study, Canadian police officers reported that Canada “does not support the global community”. This opinion points to a perceived disconnect between the stated Canadian international objectives and the realities of Canadian officer experiences.

The II World Congress against Commercial Sexual Exploitation of Children (2008) demanded that all countries to adopt legislation that prohibited the production, exhibition, and possession of child pornography (Healy, 2004). It also called for a system-wide approach of cooperation and effective relationships across private and public enterprises, borders, and jurisdictions. The International Labour Organization stated international cooperation is of particular significance to the worst forms of child labour that are transnational, such as the trafficking of children for the purposes of sexual exploitation. The 2007 Council of Europe Convention on the Protection of Children discussed the importance of international cooperation to criminal activities committed by means of a computer system and the collection of evidence in electronic form, including images of child abuse. (Newell: 2008, 11-17).

The III World Congress further called for the adoption of legislative measures and compliance with the international obligations including the enactment of legal provisions for the protection of victims. The attendees at this latest world summit recommended the

conclusion of bilateral and multilateral agreements among and between states, coordinated activity among stakeholders, and consistent law enforcement. Attendees called for a ‘strengthening of cross border and internal cooperation of law officials including “prevention, detection, investigation, prosecution and punishment” (Rio de Janeiro Declaration and Call for Action, 2008: 2). The Congress set at outcome date of 2013 to establish concrete mechanisms to facilitate coordination at national, regional and international levels for broad and enriched cooperation. (Rio de Janeiro Declaration and Call for Action, 2008: 11).

According to Grabosky (2007), it is essential that [legal] systems at least be able to keep up with the criminal exploitation of emerging technologies. He argued that the global nature of cyberspace meant that a significant amount of high technology crime would be committed trans-nationally which posed substantial challenges to law relating to jurisdiction, mutual legal assistance, and extradition. The proposed amendments to the Mutual Legal Assistance in Criminal Matters Act, announced in June 2009, claimed to widen the scope of assistance Canada provides to its treaty partners in fighting serious crimes at the international level (Justice Canada, 2009) and addressed one of the key recommendations made by the Canadian Association of Police Boards in 2008 (CABP, 2009: 15).

The Centre for Innovation Law and Policy at the University (CILP) of Toronto identified collaborative integration as one of several key recommendations to provide effective responses to the problem of child pornography on the Internet. Other

recommendations included: developing mutual legal assistance treaties to facilitate the use of evidence gathered by foreign law enforcement services; investigative information sharing; resources and training for police and prosecutorial services; police training regarding work with victims, offline child abuse prosecution, and young offenders; training of special prosecutors; and collaboration with the private sector ISPs. Finally, CILP called for legislative reform, including mandated reporting and disabling access, and educating children and the public about child pornography (Centre for Innovation Law and Policy, 2005). The pending legislation, while addressing some legislative reform, does not address mandated reporting and disabling access.

In the United States, the International Centre for Missing and Exploited Children (ICMEC) claimed that general consensus exists that global partnerships and international law enforcement collaboration are needed to effectively address images of child abuse on the Internet (Wells, 2007: 3). The ICMEC called for cooperation across law enforcement and industry that included education, standardized response mechanisms, and criminal compliance programs specific to a country's law. The G8 Ministers demanded that the "international community has to unite to create an international legal framework against child pornography that includes the United Nations' Optional Protocol to the Convention on the Rights of the Child, and the Council of Europe Convention on Cybercrime" (MOFA, 2007: 8).

In June 2009, a Justice Canada news release announced pending legislation stating that:

The global reach of cybercrime and the transnational nature of organized criminal activity in this area reveal that international cooperation is a necessity in many investigations. The proposed legislative amendments would also create the legislative framework necessary for Canada to ratify the Council of Europe's Convention on Cybercrime and the Additional Protocol to the Convention on Cybercrime. Additionally, the new legislation would include amendments to the Mutual Legal Assistance in Criminal Matters Act to broaden the scope of assistance that Canada provides to treaty partners in fighting serious crimes, including computer and computer-related crime, at an international level (Justice Canada: 2009).

The legislation does not point to new objectives, but reflects the commitments Canada made when signing the Council of Europe Convention on Cybercrime, the ILO Convention on the Elimination of the Worst Forms of Child Labour, the Convention on the Rights of the Child, and the Optional Protocol. These international instruments, along with the national laws protecting children's rights, and provincial laws overseeing child protection and child labour, contribute to safer societies for children. Enacting the pending Canadian legislation would create a legislative context through which full ratification of the Council of Europe Convention could occur, followed by any resultant enforcement. This legislation will further strengthen Canada's fight against child exploitation and its implementation would also create greater flexibility in the exchange of information critical to child rescue across agencies internationally.

Much of the EU Convention is rooted in facilitating the exchange of intelligence and supporting international investigations in operational ways; ratification will enrich the opportunity for this to occur in more efficient and effective ways. In a very real sense, the pending legislation would create a formal commitment to work operationally, to achieve

the objectives struck in Budapest almost a decade ago, and entrench the international instruments in applied practice.

Canada's law must be changed to embrace the reality of the international context: children everywhere must be protected, offenders must be pursued vigorously, and children must be rescued and rehabilitated. It is therefore recommended that Canada work harder with its international law enforcement partners and legislators to harmonize laws, facilitate intelligence exchange, and provide investigative resources by ratifying the Council of Europe Convention of Cybercrime.

Notwithstanding the international agreements that have existed for decades, without effective implementation and enforcement, treaties, conventions and agreements cannot stand alone. In the battle against child exploitation, meaningful implementation and effective policing are equally important. Effective implementation means that countries and governments must be held accountable to the responsibilities articulated in the agreements they have signed, and police throughout the world must work actively and cooperative to eradicate this crime. Treaties and conventions that are simply parchment, not practices, and laws without enforcement, are simply toothless.

## **2. National and International Synchronized and Interoperable Systems**

Since the introduction of the Internet, the volume of child sexual abuse images has grown exponentially. It is now estimated that there are over 5 million unique child sexual abuse images on the Internet (OFOVC, 2009). These world-wide figures, and the large number of countries from which these images originate gave rise to

recommendations that demanded a collaborative, effective, and international response. This demand, however, is not new. Five years ago, Snavely, Taxman, and Gordon identified the need to provide a comprehensive offender process tracking system, common platforms and closed systems, and a multi-organizational system with the ability to electronically access and exchange information (Snavely, Taxman, & Gordon, 2005). “If we are really serious about making the Internet a safer place for children, we need to secure the cooperation of a wide range of industry players, many of whom are not based in the U.K. and would be beyond the reach of national jurisdiction” (Byron, 2008: 9).

Interpol called for law enforcement agencies to establish integrated National Central Reference Points (NCPRs) to facilitate the prevention and prosecution of cybercrime. They claimed that the creation of a network of NCPRs using Interpol’s secure global communications system, I-24/7, would enable police anywhere in the world to immediately identify and obtain assistance from experts in other countries with respect to online crime investigations (Interpol, 2007). On this point, one survey respondent stated that “there needs to be a national strategy on all aspects of this issue. Training is lacking and the law does not support the global community. Interpol should provide the global coordination of investigations in an easily accessed manner”. Attendees at the III World Congress stated their support for the Interpol international child abuse images database and called for national focal points in participating countries in order to strengthen its effectiveness and adopt multilateral agreements for police investigative work (Rio de Janeiro Declaration and Call for Action, 2008: 12).

The importance of system interoperability is linked to investigative efficiency and response times (thus aiding in the rescue of children). It is helpful, claimed Interpol, to have image databases that identify what child images are already 'known' and which are new, or which have identifying background features, especially when the children have aged to the point they no longer look like the children in the original photos. When different systems use different operating protocols, or recognize different features of images, investigations are stalled. Conversely, when systems collectively recognize the serial numbers of the cameras used, can identify the location of where the camera was produced and sold, and can log the GPS location of where the photo was taken (now imbedded automatically in some digital cameras), investigations can proceed much more readily.

At the assembly of police forces from across Canada in June 2009, Anders Perrson, a Swedish police officer seconded to Interpol, announced a new Interpol-based image database, named ICSE, to replace the previous database which was only searchable by operators at Interpol. The ICSE database is relational and is searchable locally by pre-approved people over the secure i24/7 connection at Interpol. As there is no international standard for operating systems or databases, it is not surprising that ICSE does not work with other programs. However, it does give national investigators direct access to Interpol's existing Child Abuse Image Database so that officers can quickly ascertain if the images they are viewing are already known, if other police jurisdictions are investigating, or if the child has already been rescued.

At the same meeting referenced above, the NCECC simultaneously announced the development of a victim identification laboratory in Canada (CACP Conference, June 2009) while the Ontario Provincial Police (OPP) announced the launch of a one year pilot of its new database program, C4P, which is interoperable with Microsoft's Child Exploitation Tracking System (CETS), but not, presumably with ICSE. This provincially-developed system catalogues still images of child abuse, but not video, which is a serious limitation.

Hetch (2008) quoted disturbing statistics that suggest that while the availability of obscene or illegal video files constitutes a relatively small percentage of materials, video files defined as paedophilic represented nearly 4 per cent. Thus, with over one million video clips available, this means a minimum 40,000 videos of children being sexually assaulted are now posted. The newly announced Microsoft product PhotoDNA does examine video material, identifying the digital footprint of images portrayed in them (NY Times, 2009). Researchers at Dartmouth have created a method to track the original 'signature' even if the image has been changed. The heretofore lack of technical capacity to analyze these materials, and the complete paucity of synchronicity across and between public and private systems are serious concerns.

It is perplexing that none of these systems are compatible with each other, international paedophile databases, or sexual offender databases, especially given that offenders operate internationally communicating and exchanging information with

relative ease, while international, national, and provincial police agencies struggle to establish working protocols among and between each other.

The benefit of standardized systems is the potential to reduce the amount of time it takes to identify an image, thus improving the potential of rescuing a child. At present, of the world's 195 countries, 187 are members of Interpol, making it the largest international policing agency on the planet. The four core functions of Interpol are the provision of a secure global police communication service, operational data services, operational police support services, and police training and development (Interpol, 2007). Each of the recommendations made in this paper relates to one or more of the core functions of Interpol. Capacity, whether it is fully realized or not, does exist when one considers the scope and reach of Interpol. In an era of reduced police resources and increased crime, Interpol is in a key position to leverage the resources of member countries collectively more effectively.

It is therefore recommended that Interpol take the lead role in developing international standards and protocols for technological interoperability of systems and databases. Further, it is recommended that such databases include victims, known paedophiles, and offenders registered on sex offenders' registries the world over.

### **3. Local, National, and International Private-Public Partnerships**

The UN Optional Protocol to the Convention on the Rights of the Child identified the need for all actors to work holistically toward solutions (UN, 2000). And, attendees at

the World Congress III (2008) claimed that the outstanding challenges in fighting child exploitation on the Internet require a multi-sectoral approach, calling for multinational agreements as well as “establishing effective cooperation”(World Congress III Outcome Document, 2008: 2). “We need to hold those that share and distribute child sexual abuse images accountable for their role and find meaningful ways to ensure the private sector is part of the solution” (OFOVC, 2009: 13). Microsoft’s Timothy Cranton (2008) claimed that the private sector and its public partners must work together to combat child exploitation and called for ‘robust information sharing’ between law enforcement agencies and the private sector. He stated that the private sector was well equipped to work with government partners to achieve that goal (Cranton, 2008). Microsoft has developed tools and processes that aim to meet these goals as part of their corporate social responsibility strategy, and other corporations must follow suit; CETS and PhotoDNA are two discussed above, and discussion on COFEE follows.

The European Council (EC, 2009) identified ten ways in which the private sector could play an active role in protecting children and preventing their exploitation. These methods include requiring cooperation and exchange of information, tracking and maintaining data files, assisting in the development of new technology, contributing to educating parents and children through their communications systems, including web pages, and working with financial institutions to track payments made for the commercial exchange of illegal materials. As key stakeholders in the communications world, internet service providers, most of which ‘bundle’ telephone (landline and cell), cable TV, and

Internet services, must be encouraged to work collaboratively within a country's legal framework to assist in eradicating child pornography on the internet.

The Cybertip.ca (2009) Analysis of Websites reported that twenty seven different types of payment schemes were available to people purchasing images of child abuse. They also reported that nearly 60 per cent of payments could be made with traditional credit cards, many with recurring charges monthly for membership in closed groups or online communities. The market for DVDs, image sets and videos was clearly evidenced by this study, and Cybertip.ca stated "the availability of commercial child sexual abuse websites underscores the market value and demand for this type of content" (Cybertip.ca, 2009: 10). A disturbing finding was that commercial websites appear to cater to the specific tastes of offenders. Nearly one quarter of Canadian websites that hosted images of child abuse sold memberships as subscriptions, and taught users how to develop and launch their own websites, places that could then go on to host fresh pictures and new images of abuse (Cybertip.ca, 2009: 2 - 47).

This type of market availability points to the critical importance of a new example of private-public partnership that is functioning well is the establishment of financial coalitions with CEOP in the United Kingdom, and the National Centre for Missing and Exploited Children (NCMEC) in the United States. These coalitions bring together major financial organizations to disallow payment instruments for the commercial exchange of images. Originating in the United States, the coalition features membership from PAYPAL (owned by EBAY), major banks, money transfer companies, and credit card companies.

The mission of the coalition members is “to disrupt the economics of the child pornography business by denying criminals the use of the legitimate international financial system “(FCACP). In the U.S. 90 percent of the payments industry are represented at the coalition table. Referred to in the U.S. as the ‘Financial Coalition Against Child Pornography’ (FCACP), the consortium has created best practices guidelines, conducted training, and participated in the III World Congress. In their 2008 Working group report, FCACP discussed ways that Internet or on-line payments are made somewhat anonymously through hosting companies, most of which either do not written content policies, or do little to enforce their policies. The FCACP best practices recommendations cover a host of topics, not the least of which is stern warnings about the burgeoning digital payment technologies. The FCACP held PAYPAL up as an exemplar and recommended that online payment companies emulate the PAYPAL model to “thwart payments for child pornography” (FCACP, 2008: 13). Some early reports claim that the existence of the coalitions has had an impact.

Hetch (2008) reported that since the launch of the financial coalitions, the price of images of child abuse has risen dramatically. He claimed that the financial institutions were only beginning to recognize the problem, including the transaction profit realized by credit card companies on each sale of an illegal image (Hetch, 2008: 3). The FCACP rightly insisted that “the model be expanded to other countries” targeting countries including the Asia Pacific (FCACP, 2008). Signy Arnason of Cybertip.ca recently stated that the effect of the financial coalitions in the U.K. and the U.S. was being felt as many commercial

pornography websites now state that payments can no longer be made in British pounds or American dollars (CACP Conference, 2009). Canada has no such financial coalition in place, and, as the third largest hosting country of websites hosting images of child abuse, this is a situation that must be addressed (Cybertip.ca, 2009: 11).

However, a collaboration gap does exist in the coalitions that Canada has the opportunity to address in its model. ISPs are not represented at the financial tables, but as key stakeholders and partners in the communication enterprise, they should be. A Canada based coalition that brings together these key stakeholders, as well as the financial institutions is an innovative step forward that must be taken.

It is now clear that 'globalization' is not simply a catch phrase related to commerce and trade. Canada boasts of how 'wired' it is compared to other nations. As an indicator of 'development', connectedness is now a critical factor. However, children everywhere must be protected from the predilections of paedophiles, and one way to achieve this goal is standardized, integrated systems, collaborations, partnerships, modern legal frameworks, and effective enforcement.

Canada signed on to the Declaration and Agenda for Action at the I World Congress in Stockholm, in 1996. At that time, the commercial sexual exploitation was a focus of debate, with a declaration made that the commercial sexual exploitation of children is a fundamental violation of children's rights where a child is treated as a sexual object, and as a commercial object. More than a decade later, Canada must live up to the commitments made at Stockholm: greater effort must be made at the local, national, and

international levels to enhance police capacities through the development of expansion of private-public partnerships in Canada.

The Canadian Association of Police Boards 2008 Report recommended the establishment of a single, dedicated collaboration and coordination centre where police, government, the private sector, and academia could coordinate their efforts. It is important that the private-public partnerships ensure that providers of communications systems participate in consultation with the law enforcement and the criminal justice community. A Canadian industry council modeled on (or in concert with) a financial coalition would create de-facto professional industry association. And, much of the infrastructure for this type of activity exists within Interpol and the member countries. Canada must continue to work through its national centre, the NCCEC, to ensure all efforts are aligned with those of the international centre. The Canadian government must extend the NCCEC mandate to develop a Canada based financial coalition and broad base industry council.

#### **4. Mandated ISO Reporting Legislation**

Both the literature review and the data from this current study highlighted that many informed people believe that the laws in Canada are not adequate to respond to the crime of child pornography on the Internet. Canadian ISPs are currently not required to report suspicious on-line activities, nor must they disclose critical information, such as the names of customers who the police are actively investigating. Consequently, police

believe that there is much more of an exchange market in illicit materials across ISP servers in Canada than reported or investigated. “Police are currently investigating crime in Canada with investigative powers that are not up to speed with new technologies. In order to keep pace with modern communications technology and give investigators the tools they need to perform complex investigations in today's high-tech world, legislation must be modernized” (Department of Justice, 2009).

Jim Gamble, the CEO of the Child Exploitation and Online Protection Centre in the United Kingdom, spoke to the social responsibility of Internet service providers by stating “you create a public place and you have responsibilities when you do that. And, you need to live up to those responsibilities, in that public place, which is frequented by children” (Gamble, 2008: unpaginated). In Canada, Vancouver-based lawyer Benjamin Perrin, commenting on the case of R. Vs. Wilson [2009] O.J. No. 1067 said “internet service providers do make a lot of money off the sharing of child pornography and they have an obligation to contribute more to eradicate child pornography than they do now” (National Post, 2007). One respondent in the current study remarked that the Canadian Protection of Personal Information in the Private Sector Act (PIPEDA)<sup>3</sup> ought to be amended to mandate ISP cooperation. Indeed, slightly more than four-fifths of respondents in the current study (81.7 per cent) indicated that Internet Service Providers only helped police when a production order or warrant was produced. One respondent

---

<sup>3</sup> An Act to support and promote electronic commerce by protecting personal information that is collected, used, or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by, amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act.

stated that “the ISPs are the biggest hindrance to investigating child exploitation on the Internet”. While some ISPs do cooperate, “30 to 40 percent of requests are still denied. As long as they [ISPs] are at liberty to decline to provide this information to police upon request, investigations can and are being impaired. In the case of child exploitation matters, the result is that many investigations cannot proceed” (OFOVC, 2009: 15). Again, it is important to note that Justice Canada has pending legislation that “would create a preservation order that would require a telecommunication service provider (TSP) to safeguard, and not delete its data related to a specific communication or a subscriber when police believe the data will assist in an investigation” (Justice Canada, 2009).

Notably, Justice Canada stated the pending of a “measure to ensure that a communication can be traced back to the initial service provider is the expedited partial disclosure of transmission data... to allow police to request the disclosure of enough transmission data to trace all the service providers involved in the transmission of specific data” (Justice Canada, 2009). This measure would “trace domestic cybercrime when criminals attempt to hide their tracks, but also enhance international cooperation in this respect. Telecommunications generally pass through many jurisdictions, and it is necessary that all partner states have the ability to quickly determine the origin of a particular transmission during investigations” (Justice Canada, 2009).

Hyde argued a decade ago that “the issue to be addressed is not whether the legislation and/or the co-operation is available, but the ease with which Internet crime or Internet abuse can be reported, and/or investigated by the police service” (Hyde, 1999:

7). Notably absent is a call for the mandated reporting of suspicious materials and activities by ISPs to either the police or their delegates. Past pieces of legislation that called for mandated reporting have repeatedly failed on the floor of the House of Commons. The arguments launched by lobbyists for the Canadian internet service providers to the Canadian Radio Television and Telecommunications Commission, including Shaw, TELUS, and Rogers, all resonate with the arguments for privacy and against government intervention.

In 2004 a leading U.K. ISP reported that in July 2004 it blocked more than *20,000 attempts per day* to access child pornography on the Internet (Quayle, 2008: 28). These crimes are explosive, as well as exploitative, and the continued demand for new images – therefore fresh victimization – illustrates how existing public policy and the law have failed to come to grips with the realities of images of child sexual assault on the Internet.

Quayle (2008) acknowledged that there are opposing views on whether ISP reporting ought to be voluntary or mandated (Quayle, 2008: 4). Privacy advocates claim there is an element of risk in society that we must live with in order to maintain our civil liberty, no matter how abhorrent a crime may be. Some say “Is child porn wrong? Yes, but we have laws to deal with it.” Michael Giest, a law professor at Ottawa University who specializes in Internet law and crimes argued strenuously against pending legislation which he claims “deputizes” the Internet Service Providers. His most recent polemic stated “there are reports that Canada is a source of child pornography websites” (Tye

News, 2009: 3). What Giest fails to mention the fact that Canada is the third largest location of websites that host images of child sexual abuse in the world. Further, the fact that in the past dozen year the number of images of child sexual assault has risen no less than 1,500% is not noted in his treatises (Cybertip.ca, 2009: 11-18).

---

The British Columbia Civil Liberties Association (BCCLA) raised the alarm of potential “witch hunts” and claimed pending legislation would leave people vulnerable to the capriciousness of police. BCCLA is quoted as saying “ someone is turned into a child porn suspect simply because someone give a tip to the ISP, website operator or E-Mail provider...a process that would be wide open to abuse ” (Xtra.ca,2009). This hyperbole dismisses the specific and diligent investigative role and responsibilities of cybertip.ca investigators prior to formal reporting mechanisms to police. The Council of Canadians stated that “Canada wants to pass ‘lawful access’ legislation so it can continue to hang out with the cool kids (or who our government considers cool) on the international stage” (Council of Canadians, 2009), presumably other countries that have worked harder to ratify international treaties. Finally, Assistant Federal Privacy Commissioner Chantal Bernier has entered the fray, suggesting that [Bill C-46] will increase powers of the police in a way that definitely impacts on privacy (Ottawa Citizen, 2009). There is no doubt that a valuable debate will continue across different communities of interest. However, the fragile human rights of children reside at the strong roots of these arguments.

---

Lopes (2008) argued that we have an individual and collective responsibility in the protection and care for the world's children. She claimed that the citizenship (i.e. civil rights) of children is continuously and severely denied by the silence of one part of the society; for example, the silence of adults on the human rights of children in their society. The fact remains that Canada is the third largest host country of websites containing images of child sexual assault, and a real understanding of the harm to children and their human rights must prevail in the polemic. Frankly, as Lopes suggested, the rights to adult privacy must not be pitted against the basic human rights of children (III World Congress, 2008).

Undeniably, however, the Canadian legal framework, where Internet service providers have heretofore not been required to report suspicious activity, has resulted in a system that exacerbates the problem of child pornography on the Internet. Therefore, it is not surprising that the Canadian Association of Police Boards, the Canadian Association of Chiefs of Police and others, including non-government agencies, have long demanded mandatory reporting requirements for child pornography and other illicit activities. While their recommendations have not been implemented, the pending approval of Bills C-46 and C-47 seem more promising than in the past.

Historically, Canada has not had great success in advancing legislation, primarily because the required legislation has been viewed by some as imposing limits on the privacy of citizens. Over ten years ago, Bill C-42 would have required service providers'

cooperation to minimize the use of the Internet for the distribution or proliferation of child pornography or the facilitation of a sexual offence involving a child. The proposed legislation would require that service providers block access to identified portions of the Internet suspected of containing child pornography. However, the bill died after first reading on the grounds of privacy concerns (Hansard, 1998).

---

The voices of privacy advocates prevailed again in 2005 and may triumph in the future. One senior police executive privately referred to the pending legislation as 'contentious'. Indeed, as soon as the 2009 legislation was announced, the Freedom of Information and Privacy Association (FIPA) responded that the legislation was "exactly what law enforcement has been demanding and privacy groups have been fearing" for years. FIPA stated that "the new legislation is being portrayed by the government and police groups as necessary to enable law enforcement agencies to catch up to the new technologies being used by criminals... but Privacy Commissioner Jennifer Stoddart and her Provincial counterparts have argued that such measures go much further than that, giving police powers they did not have in the past, and should not have today" (FIPA, 2009:1).

---

However, from the child protection and rescue point of view, it can be argued that the recommended legislative changes announced by Justice Canada in June 2009 do not go far enough. The change child protection advocates call for is an amendment to ensure that any Internet Service Providers operating in Canada be required by law to

report suspicious materials, to retain data for a reasonable period of time, and to comply with requests for information from the police promptly. In the coming months, lobbying by special interest groups advancing the privacy agenda may result in a watered down piece of law that further hobbles effective enforcement.

The recently released “Every Image, Every Child” report referenced an important gap in Canada’s legislation, namely that suspects could not be charged with a federal offence for refusing to provide a password or encryption code upon a judicial order. It is important to remember that the offender profile, as identified by behavioral scientists at CEOP, indicated a predominance of IT professionals — those who know how to encrypt their files— committing crimes against children facilitated by technological expertise. This is just one example of where legislation is not consistent across all federal Acts. A Border Services officer can seize a computer and compel the owner to reveal encryption codes and passwords, while a police officer cannot (NOVOC, 2009). The OFOVC demanded that this loophole be closed, recommending that the federal government introduce legislation to amend the Criminal Code to make the refusal to provide a password or encryption code upon judicial order a criminal offence (OFOVC, 2009). This amendment would bring Canada’s law into accord with the United Kingdom and Australia. In both the U.K. and Australia, suspects are compelled to reveal their passwords or encryption keys or face additional charges and have their computers seized. Even if they refuse to do so, their conviction for failing to comply results in a criminal record and possible placement on the

sexual offender registry; steps which effectively impede future international travel to some countries and working with children in most.

Simply put, police in Canada must be given the legislative authority to access and examine evidence and to search computers, external hard-drives, flash-drives, USB storage devices, internet accessing gaming consoles, digital televisions, cameras, cell phones, GPS systems in vehicles, and any other type of electronic device capable of producing, storing, and/or exchanging digital images and video. As technologies emerge and converge, the need for police forensic expertise will grow even at the patrol/recruit level. This growth will place additional strain on a system which already experiences extensive backlogs for all Canadian child pornography cases. Legislative barriers, at the very least, must be eradicated. The efforts of police to rescue children and reduce sexual exploitation must not be unduly hampered by what appears to be legislative 'red tape' and pandering to an agenda set by advocates for privacy. In order to be relevant, fair, and just, the law must continue to evolve and adapt to rapidly changing societal mores and realities. In balancing offender [privacy] rights and children's rights, the overarching human rights of children must always prevail; there is no constitutionally protected right to view child pornography.

As recently as September 2009, the Canadian Federal government announced its intention to do just this, following in line with the three Canadian provinces that make reporting mandatory under provincial child protection law. The new bill, entitled "An Act respecting the mandatory reporting of Internet child pornography by persons who

provide an Internet service” is on the heels of two other related pieces of legislation: Bill C 46, “Investigative Powers for the 21<sup>st</sup> Century Act” which provides for data preservation and production orders, and Bill C47 “the Technical Assistance for Law Enforcement in the 21<sup>st</sup> Century Act that, if passed, will allow police to more readily acquire customer information from ISPs (Vancouver Sun, 2009)

It is recommended that the Government of Canada enact Bills C-46 and C-47 to include provisions for the mandatory reporting of suspicious websites, materials, and activities by Internet Service Providers including the retention of data for evidentiary purpose.

## **5. Local, National, and International Police Training**

Speaking at a world congress on the sexual exploitation of children nearly a decade ago, Carr (2001) made recommendations on the training and education of the police and the broader criminal justice system. In particular, Carr emphasized standardized law enforcement and investigative procedures, resources for police and agencies, including harmonized hotlines and databases, and codes of practice. Graham (2000) also recommended several steps that would serve to rid the Internet of child pornography, including increasing cyberspace patrols, providing better police training, and using universal crime enforcement jurisdiction. Jewkes and Andrews (2005) recommended updated legal frameworks, changes to international law, greater cooperation with private industry, and a single point for reporting and resources. They

further recommended updated forensic and investigative tools and high tech crime units. Years later, the World Congress III, in 2008, identified that “insufficient resources are made available,” and that “consistent law enforcement and the ending of impunity is often hampered by the lack of adequate resources, structures for implementation and a lack of appropriate training” (World Congress III Outcome Document, 2008: 3).

The Multi-State Working Group on Social Networking of States Attorneys of the United States stated that “greater resources should be allocated to law enforcement for training and developing of technology tools to enhance law enforcement officers’ computer forensic skills, to develop online undercover operations, and to enhance community policing efforts to educate minors, parents, and communities about youth online safety” (Berkman Centre for Internet and Safety, 2000: 37). The Virtual Task Force, a vital partner to NCCEC, called for knowledge databases, educational programs, manuals for investigators, research, information exchange, and cross sector agreements and training models (VGT, 2005). The Canadian Association of Police Boards has also called for increased funding, as well as a centralized mechanism for reporting cybercrime. Inter-provincial, national, and international cooperation is, therefore, required to establish uniform training and certification. Some respondents to the current study called for a national unit to provide a uniform approach to funding and training. They pointed to a three part strategy to hire, retain, and constantly retrain personnel.

Notably, private-public partnerships have resulted in the development of technology tools for use by first responders. In the Fall of 2009, Microsoft, in partnership

with Interpol and the National White Collar Crime Centre (NW3C) in the U.S., and Interpol, announced the launch of COFEE which is a USB device that automates one hundred fifty forensic commands on a live computer system suspected of holding illegal content. Officers can easily store and safely save digital evidence without powering down or retrieving computers physically. Universities offering degrees in cybercrime, such as University College, Dublin, have already launched programs that incorporate COFEE into their programs, and INTERPOL announced an agreement that makes COFEE available to INTERPOL member countries (INTERPOL, 2009). To date training on COFEE has not become available in Canada.

Security Watch recommended that “IT police should get a high level of technical, legal, and international training” and claimed that “reinforced and efficient international cooperation is one of the most needed solutions against cybercrime” (Security Watch, 2006: 54). For Canada, it is recommended that the National Coordination Child Exploitation Centre become the single Canadian focal point for establishing standards, education, and training certification, and that this Centre take the lead in establishing how law enforcement agencies cooperatively work with each other, the community, ISPs, and industry associations. This mandate must be pan-Canadian. In effect, the NCCEC must provide a formal, certified curriculum in cooperation with the Canadian Police College.

The Integrated Child Exploitation Units (ICE) which exist in some provinces, need to exist in all provinces. Further, not unlike complementary and augmented services between municipal forces for policing such as emergency rapid response, ICE units need

to integrate policing of on-line crimes, including images of child abuse on the Internet. It is reasonable to expect that single, isolated, or rural detachments or services cannot 'go it alone' in fighting this ubiquitous international phenomenon. Indeed, as is the case in Romania, integrated policing and child protection services could be co-located to ensure the most rapid response to child rescue. Integration and cooperation across the continuum of services to a community only serves to strengthen prevention and enforcement.

The Canadian Federal Ombudsman for Victims of Crime called for "an expansion of the National Child Exploitation Centre's National Victim Identification's Unit and support for the national database" (OFOVC, 2009: 19). Notably, the Canadian government announced that it will strengthen the laws of Canada by including a new offence to prohibit anyone from using a computer system, such as the Internet or a social networking site, to agree or make arrangements with another person for the purpose of sexually exploiting a child. This amendment, if passed, would change the current law that prohibits anyone from communicating directly with a child for the purpose of facilitating child sexual exploitation (Justice Canada, 2009). The importance of this legislation is that it creates the framework for future laws to include the many social networking practices of youth, and tackles crime in the technology playgrounds where children and paedophiles meet. CEOP (2008) reported that individuals with a sexual interest in children exploit social networking sites to collect and manage young contacts. Evidence suggests that children are victimized by adults, as well as peers, on these sites. In fact, CEOP

claimed that victims of the most serious and severe grooming behaviors, where there has been no contact sexual abuse, demonstrated the same indicators of the effect of abuse (i.e. trauma) as contact abuse victims. And, they also claimed there is little therapeutic support for children who are the victims of online offending (CEOP, 2008). In order to protect children, an effective global legal framework, that recognizes the breadth and complexities of the merging and emerging technologies, must be developed, implemented, and supported.

Advances in the UK to ensure the safety of children are dynamic while in Canada there appears to be a more passive approach. For example, in the UK, the Byron report of 2008 has already resulted in the development of new codes of practice by ISPs in the United Kingdom. These feature guidelines that concentrate on websites moderated by staff, such as chat rooms, instant messaging, and search websites drawn up by the UK Council for Child Internet Safety. Further, an educational website run by the Child Exploitation and Online Protection (CEOP) centre has designed curriculum that focuses on staying safe online that will become part of public school programs starting September 2011 (Times Online, 2009). Canada too needs to advance its relationship with educators and child protection advocates, and take similar, bold steps.

Some of the major challenges facing the implementation of the recommendations made in this paper involve interest-based people, organizations (public and private), and countries. The legal framework in developed nations is rooted in culture and often religion. Despite the collaborative appearance of the European Union, issues around

discussions of sovereignty abound. Work to develop international agreements, legal harmonization, and assistance is a massive undertaking, but it is one that the Council of Europe and Interpol have taken on and continue to champion. The interoperability of systems that allow police officers and their technologies to readily and easily exchange information on a 24/7 basis will require international standardization. Given the world's time zones and many languages, as well as the existing infrastructure, Interpol as the centralized agency makes sense. Advocates at the World Congress III called for a more active role of Interpol, where data bases of websites and uniform standards of data would be struck, and international exchange would occur (World Congress III Outcome Document, 2008: 7). The inclusion of internet service providers, financial institutions, the police in private-public partnerships in developing systems, protocols, and practices designed to eradicate child pornography facilitated by any technological means is crucial. The barriers to this recommendation are the lobbying and advocacy of the privacy agenda and the fear of the private sector that they will lose money or customers. Given this fact, partnerships must ensure that the cost of doing business the right way costs less than fines for non-compliance.

Without doubt, the most contentious recommendations in this paper are the calls for mandated reporting and ISP cooperation. However, according to Moore (2008) "the ISP is often the only entity that can identify customers in the real world". It is critical to remember that in the U.K. and elsewhere, the reporting hotlines are not staffed or operated by police. The hotlines' staff (trained civilians) establishes, through their own

investigation, if there is illegal content, and only then report to the police. Internet service providers must be compelled toward a greater sense of national and international social responsibility and report suspicious activities being conducted on the services they provide and make profit on. Further, when contacted by police, providing a customer name and address must be provided. Nonetheless, proper judicial orders for search warrants must still be obtained through appropriate means.

The training of police in Canada is an investment that will result in a greater number of cases cleared by charge, less backlog, a reduction in officer stress, and more children rescued from abuse. The training must be delivered to international standards and reflect internationally recognized competencies. Organizations, such as Bramshill in England, the Canada Police College and NCCEC in Ottawa, and Quantico in the U.S., could work proactively with Interpol, the private sector, and standards organizations to begin this process.

Anecdotally, a gap in communicating the dangers of the internet to Canadian children was observed during the research process. By way of example, CEOP in the U.K. is front and centre with public information, the development of tools for officers, and all manner of child specific on-line programs and tools. Further, the Association of Chiefs of Police in the U.K. has specific senior officers who specialize in emerging trends, such as 'cyber bullying'. Not a week goes by in the U.K. without a news item on how cyber crimes including 'child pornography' are being tackled in the U.K. from "Think You Know" campaigns for kids to advice on Christmas on-line shopping and credit card phishing and

theft. Communications conducted privately with associations and non-government organizations in Western Canada convinced the author that so much more could be done.

While arguments could be advanced against each of the recommendation made in this paper, the objectives here were to identify the major challenges that Canadian police officers perceived in stopping child exploitation, to identify capacity gaps, and to make recommendations that would address these gaps. Put in this context, the public, the private sector, and the advocates for and against privacy are encouraged to work with their policing partners to develop and support initiatives that will result in increased child rescues and the eradication of the sexual exploitation of children by adults.

## Chapter Four: Conclusion

This paper outlined the major obstacles and concerns of police officers on the capacity of Canada's law enforcement community to respond to the crime of child pornography on the Internet. The recommendations discussed in this major paper were informed by the current state of the literature, the results of a recent pan-Canadian survey, and personal notes taken by the writer at professional conferences held in Canada, Thailand, and Britain since 2008. The current study was enriched by the personal comments and observations of Canadian police officers. Many officers were clearly passionate about the issue and expressed frustration with the current state of their police organization's capacity to respond to child pornography on the Internet. For example, one officer wrote that police management only provided 'lip service' to child pornography and stated that "without money and staff, investigations are seriously impeded". Similarly, another respondent claimed "we do not have enough resources to deal with our own problems – how can we deal with issues such as child pornography that quite often occurs in other countries?"

The recommendations that are presented for Canada, by this paper, harkens back to the observations made by the United Nations Optional Protocol announced a decade ago. Actions, as identified by the UN must be holistic, strengthen global partnerships among all actions, improve policing at national levels, and integrate and ratify existing international legal instruments.

The recommendations also reflect the current academic thinking of world experts such as Ethel Quayle. Quayle (2008) speaking at the III World Congress called for an amendment to extant law in order to reflect emergent realities, including the criminalization of 'viewing' images of child sexual abuse. While she strives to differentiate between exploitive behaviours and sexual assault she called for the protection of all victims, and demanded that criminal justice systems globally respond in compassionate, accountable, and responsible ways (Quayle, 2008:104).

Importantly, regardless of the country of origin, the research and literature review conducted for this major paper confirmed the broadly held concerns of police and police researchers around the globe. Indeed, whether one speaks to an officer in rural Québec, a child protection worker advocate on Patong Beach, Thailand, or an academic from London, England, the call for increased resources, training, and legal reform remain the same. Ratifying the Council of Europe Cybercrime Protocol will go a long way towards the harmonization of international law and criminal justice practices. Ratification will create the framework for countries to move toward greater protection of children and greater enforcement capacity. Having Interpol take a leadership role by advancing their four existing core functions, in this writer's opinion, offers greater opportunity for victim identification and child rescue.

In Canada, the recommendations made by the National Office of the Victims of Crime must be championed by parliament by means of legislation. Despite arguments for privacy protection, a concerted effort must be made to empower the rights of children,

while not eradicating those of law abiding adults. Cybertip.ca or Cleanfeed, and other non-governmental child protection advocacy organizations, must work with the private sector partners and police to develop protocols that ensure Charter Rights are respected, but that offenders can be identified and punished. Notwithstanding any other rights or freedoms, child human rights must transcend all others.

The children of the world have long been exploited by adults in labor, in sex tourism, and in images of child abuse. They are abused by siblings, parents, step-parents, caregivers, and strangers. They are abused around the globe for the gratification of adults. They are scarred and traumatized not only by the original act of sexual assault, but victimized every single time their image or the image of another child is viewed. They live knowing that a permanent record of their most horrifying moments have been recorded and Retrieved by strangers; predominantly men between the ages of 26-45 (CEOP, 2008). These children have been used as commodities or as objects of sexual arousal, and this abuse must stop.

In conducting the research for this major paper, many fine and committed individuals were met, and they provided insight in untold ways. Regardless of the capacity gaps, the legislative failures, the lack of systems compatibility, there is group of committed individuals around the globe working toward protecting children. Their passion, will, energy, and sheer determination cannot be understated. Clearly, more work must be done. Research on offender profiling and treatment must continue. Children rescued from abuse must be rehabilitated. Police officers need to be supported and

counseled appropriately. The courts and judiciary must be educated on crimes facilitated by high technology. Financial institutions must collaborate and the Internet Service Providers must contribute as corporate citizens and start working more directly with law enforcement.

## References

- Berkman Centre for Internet and Safety. (2008). *Enhancing On Line Safety and Technologies*. Harvard.
- Byron., T. (2008). *The Byron Review Action Plan*. U.K. Home Office. London, U.K.
- Casey, Eoghan. (2004). *Digital Evidence and Computer Crime*. London: Academic Press.
- Centre for Addiction and Mental Health. (2009). *Child Pornography Offenders and Risk Factors for Future Offences Study*. Retrieved July 23, 2008 from [www.camh.net](http://www.camh.net).
- Centre for Innovations Law and Policy. (2005). *White Paper: Safely Connected: Strategies for Protecting Children and Youth from Sexual Exploitation Online*. Toronto.
- Child Exploitation and Online Protection Centre. (2008). *Strategic Overview 2007-2008*.
- Cooper, Sharon. (2006) Opening Oral Testimony for the US Senate Committee on Commerce, Science and Transportation.
- Congressional Research Service. Library of Congress. (2006) *Cybercrime: The Council of Europe Convention*. Washington.
- Conlon, Audrey. *Internet Advisory Board Chairwoman's Preface*. ISPAI . Retrieved July 23, 2008 from [www.hotline](http://www.hotline).
- Council of Europe (2007). *European Committee on Crime Problems: Council of Europe Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse*. Strasbourg.
- Correia, M.E. & Bowling, C. (1999). *Veering Toward Digital Disorder: Computer-Related Crime and Law Enforcement Preparedness*. *Police Quarterly* Vol. 2 No.2, June 1999 225-244.
- Canadian Centre for Justice Studies. (2002). *Cybercrime: Issues, Data Sources, and Feasibility of Collecting Police-Related Statistics*. Statistics Canada. Ottawa.
- Council of Canadians. (2009) Retrieved December 8, 2009 from [//www.canadians.org](http://www.canadians.org).
- Council of Europe. (2007). Retrieved March 15, 2008 from <https://wcd.coe.int>.

- Council of Europe (2009). Retrieved June 20, 2009 from <https://wcd.coe.int>.
- Criminal Intelligence Service Canada (2004). *Annual Report on Organized Crime in Canada*. Ottawa.
- Cojocarasu, D.I. Internet child pornography. Legile Internetului. Retrieved August 22, 2007 from [www.legi-internet.ro/index.php/Internet\\_child\\_pornography/](http://www.legi-internet.ro/index.php/Internet_child_pornography/)
- Cybertip.ca (2009). *Child Sexual Abuse Images*. An Analysis of Websites by cybertip.ca Retrieved from [www.cybertip.ca](http://www.cybertip.ca) November 25, 2009.
- Davidson, J. (2007). *Current practice and research into internet sex offending*. Risk Management Authority. Paisley, U.K..
- Darlington, Roger (2007). *Sex on the Net*. Retrieved May 6, 2007 from [www.rogerdarlington.co.U.K./index.shtml](http://www.rogerdarlington.co.U.K./index.shtml).
- Deloitte & Touche LLP. (2008). Canadian Association of Police Boards. *A report on cybercrime in Canada*. Ottawa.
- ECPAT CANADA (2006). *Global Monitoring Report on the status of action against commercial sexual exploitation of children*. Bangkok.
- ECPAT (2006). *Report on the status of action against commercial sexual exploitation of children*. Bangkok.
- ECPAT U.K. (2006). *The end of the line for Child Exploitation: Safeguarding the most vulnerable children*. London.
- ECPAT Russia (2004) Russia. *Russian National Consultation on the Commercial Sexual Exploitation of Children*. Moscow.
- Egovmonitor. Retrieved November 14, 2007 from [www.egovmonitor.com](http://www.egovmonitor.com).
- Europa. *Activities of the European Union. Summaries of Legislation*. Retrieved January 14<sup>th</sup>, 2008 from [www.europa.eu/scad/plus/leg/lvb/133116.htm](http://www.europa.eu/scad/plus/leg/lvb/133116.htm).
- European Commission (2007). *Safer Internet and eContent* Directorate-General for Information Society and Media. Luxembourg.

- European Committee on Crime Problems, *Recommendation 1778 Child Victims: Stamping out all forms of Violence, Exploitation and Abuse*. Retrieved April 15, 2007 from [www.coe.int/cdpc](http://www.coe.int/cdpc).
- Europol (2006) *Child Abuse in relation to Trafficking in Human Beings*. Factsheet 2006.
- Ferraro, M.M. & Casey, E (2005). *Investigating Child Exploitation and Pornography*. Elsevier. Amsterdam.
- Financial Coalition Against Child Pornography. (2008) *Technology Challenges Working Group Report 2008: Trends n Migration, Hosting and Payment for Commercial Child Pornography Websites*. Retrieved December 9, 2009 from [www.missingkids.com/en\\_US/documents/FCACPTechnologyChallengesWhitePaper5-08.pdf](http://www.missingkids.com/en_US/documents/FCACPTechnologyChallengesWhitePaper5-08.pdf).
- Freedom on Information Association. (2009). "Lawful Access" in Canada: Police Power to Monitor Electronic Communication." Retrieved June 18, 2009 from [www.fipa.bc.ca](http://www.fipa.bc.ca).
- Ferens, M. (2004). *An Evaluation of Canada's Child Sex Tourism Legislation Under International Law*. Faculty of Law, Manitoba. Retrieved December 9, 2009 from [www.beyondborders.org/wp/wp-content/uploads/2009/06/child-sex-tourism-paper-melissa-ferens.pdf](http://www.beyondborders.org/wp/wp-content/uploads/2009/06/child-sex-tourism-paper-melissa-ferens.pdf).
- Gamble, J. (2008) *The Child Exploitation and Online Protection Centre responds to request about Internet Service Provider (ISP) Costs*. Retrieved February 2, 2009 from [www.ceop.gov.U.K.](http://www.ceop.gov.U.K.)
- G8, Ministers of Interior, (2007). *Declaration Reinforcing the International Fight Against child pornography*, Germany. Retrieved May 30, 2008 from [www.bmi.bund.de/nn\\_122730/Internet/Content/Nachrichten/Pressemitteilungen/2007/Einelseiten/G8\\_Muenchen\\_Ministererklaerung\\_Kinder\\_en.html](http://www.bmi.bund.de/nn_122730/Internet/Content/Nachrichten/Pressemitteilungen/2007/Einelseiten/G8_Muenchen_Ministererklaerung_Kinder_en.html).
- Gillespie, A. A. (2004). *Tackling Grooming*. The Police Journal, Vol. 77. pp 239-240. [Tolley Publishing Company Ltd.](http://www.tolley.com), Croydon, U.K.
- Govender, Advaita, *Child pornography in the Age of the Internet*. Retrieved May 19, 2008 from [www.hsrc.ac.za](http://www.hsrc.ac.za).

Government of Canada, Department of Justice. Retrieved June 18, 2009 from [http://www.justice.gc.ca/eng/news-nouv/nr-cp/2009/doc\\_32388.html](http://www.justice.gc.ca/eng/news-nouv/nr-cp/2009/doc_32388.html)

Government of Canada, Health Canada. Retrieved September 13, 2007 from [http://www.phac-aspc.gc.ca/ncfv-cnivf/familyviolence/pdfs/2006-Child%20Maltreatment\\_Overview\\_English.pdf](http://www.phac-aspc.gc.ca/ncfv-cnivf/familyviolence/pdfs/2006-Child%20Maltreatment_Overview_English.pdf).

Government of Canada, Office of the Federal Ombudsman for Victims of Crime, *Every Child, Every Image*. June 2009. Ottawa

Government of Canada, Treasury Board. Retrieved September 13, 2007 from [www.tbs-sct.gc.ca/est-pre/20052006/RCMP-GRC/RCMP-GRCr5602\\_e.asp](http://www.tbs-sct.gc.ca/est-pre/20052006/RCMP-GRC/RCMP-GRCr5602_e.asp).

Graham. W.R. (2000). Uncovering and Eliminating Child Pornography Rings on the Internet: Issues Regarding and Avenues Facilitating Law Enforcement's Access to 'Wonderland'. *The Law Review of Michigan State University*.

Harrison. C. (2006.) Cyberspace and Child Abuse Images: a feminist perspective. *Affilia: Journal of Women and Social work* 21 (4): 365-379. Howard University Press. Washington.

Hetch, M. (2008). *Private Sector Accountability in Combating the Commercial Sexual Exploitation of Children*. International as a contribution to the World Congress III against Sexual Exploitation of Children and Adolescents. Retrieved December 10, 2009 from <http://www.iiicongressomundial.net>.

Healy, M. A. (2004). *Child pornography: An International Perspective*. World Congress against Commercial Sexual Exploitation of Children. Stockholm.

Henschel, B. (2003) *The Assessment of Commercial Sexual Exploitation of Children: A Review of Methodologies*. Understanding Children's World. UNICEF, World Bank, IMO. Retrieved December 4, 2009 from [www.childtrafficking.com](http://www.childtrafficking.com).

Hodgson J.F. and Orban, C. (2005). *Public Policing in the 21<sup>st</sup> Century*. Criminal Justice Press. New York.

Holland, G. (2005). *Identifying victims of child abuse images; an analysis of successful identifications*. In E. Quayle and M. Taylor (2005). *Viewing Child Pornography on the Internet. Understanding the Offence, Managing the Offender, \helping the Victims*. Lyme Regis: Russell House Publishing. London.

Hyde, S. *A Few Coppers Change*, (1999). *The Journal of Information, Law and Technology*. The Law School. University of Warwick, U.K.

ICE, US Immigration and Customs Enforcement. Retrieved February 28, 2009 from <http://www.ice.gov/pi/nr/0902/090209boise.htm>

ICMEC. 2006. *Child Pornography: Model Legislation & Global Review*. ICMEC. Alexandria.

International Labour Organization (ILO). *Convention 182 on the Worst Forms of Child Labour*. Retrieved December 1, 2009 from [http://www.ilo.org/global/About\\_the\\_ILO/Mission\\_and\\_objectives/lang--en/index.htm](http://www.ilo.org/global/About_the_ILO/Mission_and_objectives/lang--en/index.htm)

INHOPE, 2009. Retrieved November 30, 2009 from <https://www.inhope.org/>.

Internet Watch Foundation (2006). *Annual and Charity Report*. London.

Internet Watch Foundation (2007). *Annual and Charity Report*. London.

Interpol. Media release. Retrieved February 10, 2007 from [www.interpol.com](http://www.interpol.com).

Interpol. Media release. Retrieved December 3, 2009 from [www.interpol.com](http://www.interpol.com).

Jenkins, Philip. (2001). *Beyond Tolerance: child pornography on the Internet*. University Press. New York.

Jewkes, Y. and Andrews, C. (2006). 'The problem of child pornography on the internet: international responses' in Y. Jewkes (ed.) *Crime Online*, Cullompton: Willan.

Jones, V (2005). Position paper regarding online images of sexual abuse and other Internet-related sexual exploitation of children. Retrieved May 6, 2008 from

Kanellia, P. (Ed) (2006). *Digital Crime and Forensic Science in Cyberspace*. Hershey, PA.

Lanning, K. (1992). *Child Molesters: A Behavioral Analysis*, Washington, DC: National Centre for Missing and Exploited Children.

Library of Congress. (2007). *Children's Rights: International and National Laws and Practices*. Retrieved December 7, 2009 from [www.loc.gov/law/help/child-rights/canada.php](http://www.loc.gov/law/help/child-rights/canada.php).

- Lopes, M. (2008) *Integrated Cross- Sector Policy*. III World Congress, Rio. Retrieved December 1, 2009 from 2009 from [www.iiicongressomundial.net](http://www.iiicongressomundial.net).
- Malinowski.C. (2006). *Training the Cyber Investigator*. Digital Crime and Forensic Science in Cyberspace. Idea Group. Hershey, P.A.
- Marshall, W. L. (2000) *Revisiting the use of pornography by sexual offenders: Implications for theory and practice*. *Journal of Sexual Aggression* 6, (1/2), 67-77. Taylor & Francis. London.
- McAfee (2008) *Cybercrime Versus Cyberlaw*. Santa Clara, California.
- McCabe, K. (2008) *The Role of Internet Service Providers in Cases of Child Pornography and Child Prostitution*. *Social Science Computer Review* 20 (2) 247-251).
- McNulty, P.J. (2007). Project safe childhood. *The Police Chief* 74 (3). Retrieved September 14, 2007 from [www.policemagazine.com/index/cfm?fuseaction=display\\_arch&article\\_id=1138&issue\\_id=32007](http://www.policemagazine.com/index/cfm?fuseaction=display_arch&article_id=1138&issue_id=32007).
- Microsoft. (2008). *Statement of Timothy W. Cranton to US Commission on Security and Cooperation in Europe*. Retrieved from [www.microsoft.com](http://www.microsoft.com) 03-12-2009.
- Middleton, D. Elliott, I.A., Mandeville-Norden R & Beech, A.R. (2006). An investigation into the applicability of the Ward and Siegert pathways model of child sexual abuse with Internet offenders. *Psychology, Crime and Law* 12(6): 589-603. Routledge. London.
- Ministry of Foreign Affairs, Japan (2001). *Report of the Second World Congress against Commercial Sexual Exploitation of Children*. Yokohama, Japan
- Mittal, S. (2004). *Child Development*, Gyan Books, India.
- Moore, Robert. (2005). *Search and Seizure of Digital Evidence*. New York. N.Y.
- Morita, A. (2008). Internet Boosts Reports of Child Pornography. Retrieved February 2, 2009 from [www.physorg.com](http://www.physorg.com).
- Muir, D. (2005). *Violence Against Children in Cyberspace*. ECPAT. Bangkok.

- New York Times. (2009) *Microsoft Tackles the Child Pornography Problem*. Retrieved December 16, 2009 from <http://bits.blogs.nytimes.com/tag/dartmouth-college>.
- Newell, P. (2008) *Legal Frameworks for Combating Sexual Exploitation of Children*. Paper presented on Legal Frameworks, Procedures and Enforcement: Preventing and Responding to Sexual Exploitation of Children and Adolescents, Bern, Switzerland October 2008, retrieved November 30, 2009 from [http://www.iiicongressomundial.net/index.php?pg=docs&inicial=2&id\\_pg=79&sid=20884c6bfaa4421fae2bfa4237e738eb&id\\_sistema=2&id\\_idioma=2](http://www.iiicongressomundial.net/index.php?pg=docs&inicial=2&id_pg=79&sid=20884c6bfaa4421fae2bfa4237e738eb&id_sistema=2&id_idioma=2)
- Organisation of American States (2003). *Technical Secretariat for Legal Cooperation Mechanism*. Secretariat for Legal Affairs. Washington.
- Organisation of American States (2000) *Final Report of the Second Meeting of Government Experts on Cybercrime*. San José, Costa Rica.
- O'Donnel I. & Milner, C. (2007). *Child Pornography*. Willan Publishing. Devon.
- Pattavina, A. (Ed). (2005). *Information Technology and the Criminal Justice System*. Thousand Oaks: Sage Publications, Inc.
- Plecas, D & Anderon, G. (2002). *Physical Evidence of Police Officer Stress*. Policing. Vol. 25. No.2.
- Quayle, E. & Taylor, M . Pornography and the Internet (2001). *Deviant Behaviour: An Interdisciplinary Journal* (pp 331-357).
- Quayle, E. (2006). *Cyberpsychology and Behaviour*, Volume 6, Number 1.
- Quayle, E. (2008). *Child Exploitation and Sexual Exploitation of Children Online*. Presented At III World Congress, Rio. Retrieved December 4, 2009 from [www.iiicongressomundial.net](http://www.iiicongressomundial.net)
- R. Vs. Wilson [2009] O.J. No. 1067
- RCMP (2007). *Virtual World, Real Crimes, Real Children*. NCECC Interim Progress Report. Ottawa.
- Rogers. M (2007). Questionnaire of law enforcement perceptions regarding digital evidence. *IFIP international federation for information processing*. 242:41-52.

- Russel, Glenn. (2003). *Training the 21<sup>st</sup> Century Police Officer: Redefining the Police Profession for the Los Angeles Police Department*. Santa Monica. Rand, Los Angeles.
- Sanderson, Christiane. (2004). *Seduction of Children: Empowering Parents and Teachers to Protect Children from Sexual Abuse*. London, U.K.
- Save the Children. (2005). *Online Images of Sexual Abuse and other Internet-related Sexual Exploitation of Children*. Copenhagen. Denmark.
- Schell, B.H. (2006). A Cyberchild pornography Case in Point. *Aggression and Violent Behaviour* Vol 12 45-63.
- Sheldon, K & Howitt, D. *Sex Offenders and the Internet*. Wiley & Son. Sussex.
- Sinclair, RL (2005) Internet Based Sexual Exploitation of Children and Youth, *Environmental Scan*. Retrieved May 7, 2007 from [http://ncecc.ca/enviroscan\\_2005\\_e.htm](http://ncecc.ca/enviroscan_2005_e.htm).
- Stol, W. Ph. (Wouter).(2002). *Policing child pornography On the Internet - In the Netherlands*. *Police Journal* (pp 45-55).
- Sutton, D. (2004) Internet-related sexual exploitation of Children. Brussels.
- Tan, Ken Hwee. (2000). Prosecuting Foreign-Based Computer Crime: International Law and Technology. Symposium on Rule of Law in the Global Village. Palermo.
- Taylor M. & Quayle, E. (2003). *Child Pornography: An Internet Crime*. Bruner-Routledge. London.
- Taylor, M & Quayle, E. Child pornography and the Internet: Challenges and Gaps 2nd World Congress Against the Commercial Sexual Exploitation of Children, Yokohama, December 2001.
- Times Online (2009). *Websites sign up to new internet standards code*. Retrieved December 6, 2009 from [www.technology.timesonline.co.uk](http://www.technology.timesonline.co.uk)
- Thomas, D. & Loader, B.D. (Eds.). (2000). *Cybercrime*. London: Routledge.

- UNICEF & UNISYS, (2003). *Child Pornography on the Internet. Evaluating Preventive Measures in order to Improve Their Effectiveness in the EU Member States*. Trento, Italy.
- United Nations. (1989). Office of the High Commission. *Convention on the Rights of the Child*. Retrieved November 30 from [www2.ohchr.org/english/law/pdf/crc.pdf](http://www2.ohchr.org/english/law/pdf/crc.pdf).
- United Nations. (2009). Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution, and child pornography. Retrieved December 8, 2009 from [www.un.org](http://www.un.org).
- U.S. House of Representatives. (2007). *Sexual Exploitation of Children over the Internet*. Retrieved February 14, 2007 from [www.access.gpo.gov/congress/house/house05ch109](http://www.access.gpo.gov/congress/house/house05ch109).
- Vancouver Sun. (2009). *Ottawa Aims to Strengthen Internet Child Porn Laws*. Retrieved November 24, 2009 from [www.vancouversun.com/news](http://www.vancouversun.com/news)
- Walker, D., Brock, D., Stuart, T.R. (2006). *Faceless-Oriented Policing: Traditional Policing Theories are not Adequate in a Cyber World*. *Police Journal*, Vol. 79.
- Wells, M. (2007). *Defining child pornography: Law Enforcement Dilemmas in Investigations of Internet child pornography Possession*. *Police Practice and Research*, Vol. 8. No. 3.
- Wood, D.S. (2007). *Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace*. *Police Practice and Research*, Vol. 8., No. 2, pp 184 -
- Wall, D.S. (2007). *Police Practice and Research: An International Journal. Policing cybercrimes: Situating the Public Police in Networks of Security within Cyberspace*. Routledge: Abington.
- Wall, D.S. (2007). *Cybercrime*. Cambridge. Polity Press.
- Wolak, J., Mitchell, J. (2009) *Work Exposure to Child Pornography in ICAC Task Forces and Affiliates*. University of New Hampshire, N H.
- Westby, Jody (Editor). (2003). *International Guide to Combating cybercrime*. American Bar Association.

## Appendix 1: Letter of Survey Completion Request

This survey is being conducted by the School of Criminology and Criminal Justice at the University College of the Fraser Valley to assess the capacity of the municipal police forces in Canada to respond to the problem of child pornography on the Internet. In particular, and from a law enforcement perspective, the survey is intended to provide information about technological, training, legal, financial, and human resource gaps in our efforts to deal with the problem of child pornography on the Internet. A copy of the final report will be provided to the Canadian Association of Chiefs of Police and any individual police office requesting one.

There are no personal or specific agency indicators in the survey and no tracking of respondents will occur. Further, all information will be aggregated and in no way will any respondent be identifiable. Accordingly, your responses will be anonymous.

The questionnaire itself should take you about ten minutes to complete. In completing it, please be reminded that you need not answer any question that you don't feel comfortable answering. Further, please add as much comment as you like in answering the last question. Once you have completed the questionnaire, you need only put it in the pre-stamped envelope provided and mail it back to us. Please do not put any identifying marks on the envelope or use envelopes that identify yourself or your organization. We are hoping to have all questionnaires returned by **February 28, 2008** at latest.

For the present, if you have any questions, please do not hesitate to call me at the University College of the Fraser Valley at 604-504-7441. For any concerns regarding the administration of the survey, please contact Yvon Dandurand, Associate VP of Research and Graduate Studies at 604-864-4654.

Ce sondage a pour but d'évaluer la capacité des corps de police municipaux au Canada de répondre au crime de la pornographie infantile d'Internet. Je m'intéresse à savoir ce que vous, policiers municipaux, pensez de la façon dont le Canada adresse ce problème, et aussi par rapport à d'autres juridictions. Cette enquête cherche à décrire l'état actuel de ce qu'on appelle souvent " les images de l'abus des enfants à l'Internet." Le résultat de cette enquête sera le développement de recommandations qui pourraient contribuer à réduire les insuffisances de ressources, de technologies et d'éducation dans le système de police canadienne tels qu'identifiées dans cette enquête.

Nous vous demandons de répondre à ce sondage parce que vous êtes un investigateur d'expérience dans ce domaine. Il n'y a aucun indicateur personnel ou communautaire dans ce sondage et il n'y aura aucun suivi avec les répondants.

Vos commentaires seraient la bienvenue et, quand c'est possible, ils seront incorporés dans le document de travail. Notez, SVP, que toutes les informations recueillies seront agrégées et les répondants ne seront jamais identifiés. De cette manière, tous les répondants demeureront confidentiels. En répondant, vous demeurerez anonyme. En plus, s'il y a des questions auxquelles vous ne voulez pas répondre, vous êtes libre de ne pas répondre. Nous vous donnons une enveloppe timbrée pour nous transmettre le questionnaire rempli. Nous aimerions recevoir votre questionnaire pas plus tard que **28 de février, 2008**.

Si vous avez des questions, SVP contactez-moi à l'University College of the Fraser Valley, au 604.504.7441. Si vous avez des questions au sujet de l'administration de ce sondage, veuillez contacter Yvon Dandurand, Associate VP of Research and Graduate Studies, au 604.864.4654.

Les services de police qui voudraient recevoir une copie de l'étude une fois complétée sont priés de contacter le School of Criminology and Criminal Justice, à University College of the Fraser Valley. Je

**Survey of Canadian Municipal Police Forces**

---

**The Capacity to Respond to “Child Pornography”  
On the Internet**



**School of Criminology and Criminal Justice**

Catherine Dawson, M.Ed. (MA Candidate)

Darryl Plecas, Ed.D.

Irwin Cohen, Ph.D.

©2008 All Rights Reserved

This document may not be reproduced in any manner, in whole or in part, without the written permission of the School of Criminal Justice, University College of the Fraser Valley

**1. Please circle the number that best describes the degree to which you agree or disagree with the following statements.**

	Strongly Disagree	Disagree	Agree	Strongly Agree
1. The laws in Canada are adequate to enable police to respond to child pornography on the Internet.	1	2	3	4
2. I believe that the police with whom I currently serve in my community have the knowledge to investigate "child pornography" on the Internet.	1	2	3	4
3. I believe that the police with whom I currently serve in my community have the skills to investigate "child pornography" on the Internet.	1	2	3	4
4. I believe that the police with whom I currently serve in my community have the financial and human resources to investigate "child pornography" on the Internet.	1	2	3	4
5. Internet service providers (ISPs) provide help to investigating police officers in my community when investigating Internet based crime, including "child pornography" on the Internet.	1	2	3	4
6. The help that Internet Service Providers (ISPs) provide is strictly by warrant or production order.	1	2	3	4
7. The officers with whom I currently serve in my community know exactly what to do with a computer and peripherals when they are the first responders to a crime scene in which computers and/or peripherals are present.	1	2	3	4
8. Specific cyber-crime training is provided to the officers with whom I serve in my community on a regular basis.	1	2	3	4
9. The cyber-crime training provided is sufficient to keep pace with technology.	1	2	3	4
10. To my knowledge, no one in my community has ever been charged under Section 172.1 of the Criminal Code.	1	2	3	4
11. There have been investigations where the geographic origin of child pornography on the Internet could not be identified.	1	2	3	4
12. Protocols for patrol officers in my detachment/department attending calls for service regarding the discovery of images of child abuse on a home, school, or office computer are in place.	1	2	3	4
13. The officers with whom I serve who investigate child pornography on the Internet regularly receive personal counselling.	1	2	3	4
14. A single, specialized <b>Canadian</b> investigation, training, and police resource unit would enrich the Canadian police capacity to respond to the crime of "child pornography" on the Internet.	1	2	3	4
15. A single, specialized <b>International</b> investigation, training, and police resource unit would enrich the Canadian police capacity to respond to the crime of "child pornography" on the Internet.	1	2	3	4

**2. Please rank order the current capacity of the following regions to respond to child pornography on the Internet. Please put a "1" next to the location with the best capacity and "5" next the location with the worst capacity.**

Region	Capacity Rank Order
1. United Kingdom	
2. South Africa	
3. Canada	
4. USA	
5. India	

**3. Please rank order your opinion on the greatest challenges you face in responding to “child pornography” on the Internet. Please place a “1” next to the greatest challenge, a “2” for the 2<sup>nd</sup> greatest challenge, and a “3” for the 3<sup>rd</sup> greatest challenge.**

	Rank Order
1. Technological capacity; we do not have the equipment we need	
2. Financial capacity; we do not have the money we need	
3. Personnel; we do not have the <i>trained</i> people we need	

**In this section we would like to gather some information on your service:**

**4. The number of police officers in the local police detachment/service in which I work:**

- 1. 1 – 50
- 2. 51 – 100
- 3. 101 – 150
- 4. 151 – 200
- 5. Over 201

**5. Does your police service have a dedicated unit for cyber crime?**

- 0. No
- 1. Yes



**6. Do you have any single officer who works specifically on cyber crime?**

- 0. No
- 1. Yes



**7. Please indicate how many members are in the unit:**

- 1. 2 – 5
- 2. 6 – 10
- 3. 11- 15
- 4. 16+



**8. Cyber crime investigations in my detachment/service is managed by:**

- 1. No one, we do not investigate
- 2. Regional units of investigators
- 3. Integrated law enforcement units
- 4. Other

**9. Is there a person specifically dedicated to the investigation of “child pornography” on the internet?**

- 0. No
- 1. Yes

**10. The approximate backlog to initiating a full investigation on a cyber crime in my service is**

- 1. 1 – 4 months
- 2. 5 – 7 months
- 3. 8 – 12 months
- 4. over 12 months

**10. The population size served by my police service is approximately:**

- 1. Under 49,999
- 2. 50,000 – 99,999
- 3. 100,000 – 199,999
- 4. 200,000 – 499,999
- 5. 500,000 – 999,999
- 6. 1,000,000 +

**11. The officers who investigate cyber crime in my community’s police service have been trained in:**

	No	Yes
Email Tracking	0	1
ISP Tracking	0	1
Covert Investigation	0	1
Evidence Gathering and Preservation	0	1
Health and Safety	0	1

Please use this space to provide any additional comments you would like to make about the capacity of municipal police forces in Canada to respond to “child pornography” on the Internet.

**Thank you for completing this survey**