



Heard. Respected. Victims First.
Écoulées. Respectées. Victimes d'abord.



Every Image, Every Child

INTERNET-FACILITATED CHILD SEXUAL ABUSE IN CANADA





OFFICE OF THE FEDERAL OMBUDSMAN FOR VICTIMS OF CRIME

In March 2007, the Ministers of Justice and Public Safety announced the creation of the Office of the Federal Ombudsman for Victims of Crime to ensure the federal government meets its responsibilities to victims of crime.

As part of its mandate, the Office identifies emerging issues that impact negatively on victims of crime and makes recommendations to Parliament based on those issues and the principles set out in the *Canadian Statement of Basic Principles of Justice for Victims of Crime*.

This report is part of that important work.



Table of Contents

Executive Summary	1	6. Helping Victims Heal	30
The Issue	2	Child advocacy centres:	
Scope of the Problem	4	A model for success	30
Impact of the Internet	4	Child advocacy centres in Canada	32
User as abuser	6	How child advocacy centres can help victims of Internet-facilitated child sexual abuse	33
Younger victims and increasing violence	8	7. Learning to Better Help Victims	34
Progress to Date	10	Answering tough questions	35
What More Needs to Be Done—		8. Ending Ongoing Victimization	37
Recommendations	13	Handling of child sexual abuse images in the Canadian justice system	38
1. Child Pornography—A Dangerous Term	14	9. Stemming the Flow of Child Sexual Abuse Images over the Internet	40
2. Rescuing Children from Internet-Facilitated Sexual Abuse	15	Working with the private sector	40
Giving authorities the tools they need	16	Conclusion	43
The right to privacy	17	Appendix 1—List of recommendations	44
Privacy rights of the victim	20	Appendix 2—Index of abbreviations	46
The need for legislative change	22		
3. Gathering Evidence—			
Disappearing Information	24		
4. Accessing and Storing Information	25		
5. Identifying Victims through Image Analysis	27		
Image databases	27		
Building expertise	28		
Responsible image management	29		



"I don't think I will call him
Daddy anymore."

—Young child abused by her father live on the Internet¹



Executive Summary

EVERY IMAGE, EVERY CHILD gives an overview of the problem of Internet-facilitated child sexual abuse, provides limited historical information about what has been done by the federal government on the issue to date, identifies issues that negatively impact child victims and makes nine recommendations for positive change.

The nine recommendations touch on:

- the term “child pornography”;
- the limitations of our current privacy laws and the dire implications these have for law enforcement agencies working to find offenders and rescue child victims;
- the importance of devoting more resources to identifying and rescuing the children found in sexual abuse images;
- the need to better understand and address the needs of children who have been identified as victims of Internet-facilitated sexual abuse; and
- solutions for reducing the distribution of child sexual abuse images.

The recommendations contained in this report are directed to the Ministers of Justice and Public Safety, the National Child Exploitation Coordination Centre of the RCMP and the Policy Centre for Victim Issues of the Department of Justice.

¹ Gregory Bonnell, “Man who sexually abused daughter live on internet sentenced to five years,” Canadian Press, December 20, 2007.



"Child pornography grievously harms all children: it harms the child who is sexually assaulted in the making of the images; the same child is re-victimized every time that image is viewed.... Because no child should be victimized in this horrific way, today we pledge to redouble our efforts to enforce the international fight against child pornography."

—G8 Justice and Home Affairs Ministers²

The Issue

GENERALLY, MORE THAN 90 PERCENT 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.³ The number of charges for production or distribution of child pornography increased by 900 percent between 1998 and 2003.⁴

Despite these clear concerns, the issue of child sexual abuse and the Internet can sometimes seem to be as difficult to discuss as to tackle. Unfortunately, we do not have a choice. We cannot afford to turn our heads or

cover our ears because the problem is growing. And it is getting exponentially worse. Images are getting more and more violent, and the children in those images are getting younger and younger.

This report provides an overview of child sexual abuse and the Internet; where we are, where we have been, the gaps that exist and what we must do to address them. Specifically, the report provides a summary of the scope of the problem, a brief history of the progress that has been made so far and, most importantly, makes nine recommendations for future changes relating to child

² G8 Justice and Home Affairs Ministers, "Reinforcing the International Fight Against Child Pornography," May 24, 2007. www.canadainternational.gc.ca/g8/ministerials-ministerielles/2007/child_porno-enfant_porno.aspx?lang=eng.

³ Canadian Centre for Child Protection, "What we know" www.protectchildren.ca/app/en/whatwek, March 25, 2008.

⁴ Only 33 percent of those convicted of distribution were sentenced to prison (52 percent received probation). Child and Youth as Victims of Crime, *Juristat*, 1, April 20, 2005, p. 11. Statistics Canada Catalogue No. 85-002-XIE.

sexual abuse images, or “child pornography,” to the Ministers of Justice and Public Safety, the National Child Exploitation Coordination Centre (NCECC) of the RCMP and the Policy Centre for Victim Issues of the Department of Justice.

These recommendations touch on the term “child pornography” itself, on the limitations of our current privacy laws and the dire implications they have for child victims, on the importance of devoting more resources to identifying and rescuing children who are abused, on properly handling victims who are identified and helping them to heal, and on the need to stop the dissemination of this horrible material.

These recommendations are consistent with the Government of Canada’s responsibilities to victims as set out in the *Canadian Statement of Basic Principles of Justice for Victims of Crime*, the *Canadian Charter of Rights and Freedoms* and the various commitments the Government has made at the United Nations and G8.

If accepted, these recommendations will both make a difference in the lives of innocent children and help make Canada a global leader in trying to identify victims and respond to their needs.





"Child pornography has...grown into a massive industry that systemically promotes the abuse of children."⁵

Scope of the Problem

Impact of the Internet

"The Internet is not 'creating a sexual interest in children' but it's creating victims!"

–Dr. Peter Collins⁶

"The menace that distribution of child pornography through the internet poses cannot be underestimated. The internet provides an unregulated, instant world-wide distribution network that is immediately accessible for viewing, downloading and even wider distribution."⁷

"We were trading pictures...kinda like trading baseball cards. There was also the thrill in collecting them. You wanted to get complete sets so it...was kind of like stamp collecting as well."

–Collector of child pornography⁸

The impact of technology and specifically the Internet on child pornography images cannot be overstated. It can be seen most strikingly in three areas: production, distribution and community. The illusion of anonymity and the near universal accessibility of the Internet enable a vicious cycle: the creation of a community of like-minded individuals

⁵ Martin C. Calder, "The Internet: Potential Problem and Pathways to Hands-On Sexual Offending," in Martin C. Calder (ed.), *Child Sexual Abuse and the Internet: Tackling the New Frontier*, 2004.

⁶ Alison Haines, "Child porn, pedophilia linked but potential offenders hard to pinpoint," Canwest News Service, March 26, 2006.

⁷ *R. v Hunt* (2002) AJ No. 831 at para. 29 (C.A.).

⁸ Ethel Quayle and Ma Taylor, "Child Pornography and the Internet," (2002) 23 *Deviant Behaviour* at 342.

Fast Facts

- Commercial child pornography is estimated to be a *multi-billion* dollar industry worldwide.⁹
- There are over 750,000 pedophiles online at any given time.¹⁰
- Thousands of new images or videos are put on the Internet every week¹¹ and hundreds of thousands of searches for child sexual abuse images are performed daily.¹²
- Offenders may have collections of over a million child sexual abuse images.
- An image of a 4-year-old girl in diapers has been shared an estimated 800,000 times.¹³
- Most child sexual abuse image producers are known to the victims:
 - ▶ 37 percent are family members.¹⁴
 - ▶ 36 percent are acquaintances.¹⁵
 - ▶ Over 30 percent of those convicted of possessing child pornography were living with minor children; almost 50 percent had access to minors at home, socially or as part of their jobs.¹⁶

who share and “collect” images, the eventual desire of those individuals to obtain higher numbers of more shocking images and finally, the willingness of members to create more violent images. Once completed, the cycle begins again. Currently, an estimated 500,000 individuals are actively involved in the trafficking of child sexual abuse images on the Internet.¹⁷

Since the creation of the Internet, the volume of child sexual abuse images has grown exponentially. Images and videos are traded like baseball cards every minute of every day, and the sheer volume is staggering. It is estimated that there are over 5 million unique child sexual abuse images on the Internet.¹⁸

⁹ Jonah Rimer, *Literature Review—Responding to Child & Youth Victims of Sexual Exploitation on the Internet*, 2007. The creation and distribution of most images is not related to commercial purposes. www.boostforkids.org/pdf/RCE-Literature-Review.pdf, p. 30.

¹⁰ Jane Sims, “So savvy...but so vulnerable,” *The Ottawa Sun*, October 12, 2008.

¹¹ Dr. Roberta Sinclair, The National Child Exploitation Coordination Centre, “Internet Facilitated Sexual Exploitation,” PowerPoint presentation made to the 2007 National Crime Victim Awareness Week Symposium, April 23, 2007.

¹² Ibid.

¹³ Suzanne Fournier, “Police outgunned by Internet perverts,” *Vancouver Province*, October 22, 2008.

¹⁴ Jonah Rimer, *Literature Review—Responding to Child & Youth Victims of Sexual Exploitation on the Internet*, 2007, p. 25.

¹⁵ Ibid.

¹⁶ Adrian Humphreys, “Predators among us—do we have an epidemic or not?,” *National Post*, October 20, 2007. These statistics refer to a study done by the National Center for Missing and Exploited Children regarding 1,713 people charged with possessing child pornography.

¹⁷ “President Bush signs child protection bill into law,” October 14, 2008. [/cbs4.com/seenon/internet.sex.predator.2.840236.html](http://cbs4.com/seenon/internet.sex.predator.2.840236.html).

¹⁸ Dr. Michael Bourke, “Child Pornography and Hands-on Abuse,” Dallas Crimes Against Children Conference, August 12, 2008.

User as abuser

"...they trade them just like hockey cards. Just like a sports fan would try to collect an entire team in a sport, they will try to collect all 20 images of this young girl. It's called a series."

–OPP Detective Paul Chambers¹⁹

On May 12, 2003, 10-year-old Holly Jones was abducted while walking home from a friend's house. Minutes before he forced her into his home, sexually assaulted and murdered her, Michael Briere was looking at child sexual abuse images online.

Briere pled guilty to first degree murder and is currently serving a life sentence. At his sentencing hearing, Briere told the court he was consumed by desire after viewing child pornography and that, "Viewing the material does motivate you to do other things. The more I saw it, the more I longed for it in my heart.... I really wanted to have sex with a child. And that was all-consuming."²⁰

Everyone who knowingly views and accesses child sexual abuse images for gratification purposes is an abuser. Whether it is the very act of degrading that child by viewing the image, or the niche market that viewers create for those producing the material, or the hands-on abuse inflicted by the offenders themselves, in each case a child is being abused.

The creation and distribution of most images is generally not motivated by commercial purposes. Some abusers take photographs so they can use them for sexual gratification in the future. Others use these sexually abusive images to groom children for future abuse or to coerce their child victims into silence. In recent years, a growing number of offenders indicated that they were motivated to produce these vile images to enhance their status with other child abusers on the Internet.²¹

There are those who may argue that viewers are "just looking at pictures." However, research suggests it is not that simple. In *R. v. Sharpe*, Chief Justice McLachlin of the Supreme Court of Canada stated that "the link between the production of child pornography and harm to children is very strong."²² According to Jonah Rimer, research assistant with the BOOST Child Abuse Prevention & Intervention Centre, more than half of child pornography offenders either abuse or attempt to abuse children.²³

Child pornography offenders average 20 victims each—more than double that of contact offenders.²⁴

¹⁹ Tracy McLaughlin, "Kid-sex pics traded like hockey cards: Cop," *Toronto Sun*, September 22, 2008.

²⁰ Julian Sher, *Caught in the Web: Inside the Police Hunt to Rescue Children from Online Predators*, Perseus Publishing, 2007, p. 38.

²¹ Michelle Collins (National Center for Missing and Exploited Children), "Child Pornography: A Closer Look," *Police Chief Magazine*, March 2007, 74(3).

²² *R. v. Sharpe*, 2001 SCC 2, [2001] 1 S.C.R. 45, para. 92.

²³ Jonah Rimer, *Literature Review—Responding to Child & Youth Victims of Sexual Exploitation on the Internet*, 2007, p. 32.

²⁴ Julian Sher, *Caught in the Web*, 2007, pp. 40–41.

Dr. Michael Bourke and Andres Hernandez (Federal Bureau of Prisons) suggest the numbers may be even higher than 50 percent. Their study, which looked at prisoners serving sentences for child pornography offences (as opposed to contact offences), found that child pornography offenders had in fact molested thousands of children, none of whom had reported the abuse.

“The dramatic increase (2,369%) in the number of contact sexual offences acknowledged by the treatment participants challenges the often-repeated assertion that child pornography offenders are only involved with pictures. It appears that these offenders are far from being innocent, sexually curious men who, through naiveté or dumb luck, became entangled in the World Wide Web...”²⁵

The study found that less than 2 percent of subjects who entered treatment without known hands-on offences were verified to be “just looking at pictures.” Instead, 85 percent of the sample admitted to being child abusers which, as the study points out, calls into question whether it is useful to discriminate between child pornographers and child abusers or even pedophiles.²⁶

Similarly, a study conducted by Toronto’s Centre for Addiction and Mental Health compared men who were convicted of molesting children and others who were convicted of possessing illegal photos. Researchers found that the offenders who were convicted of the possession offences had a higher chance of exhibiting a pedophile attraction to children than men who actually molested children. Dr. Seto wrote, “Our results indicate that child pornography offending is a valid diagnostic indicator of pedophilia.... In fact, child pornography offenders, regardless of whether they had a history of sexual offences against child victims, were more likely to show a pedophilic pattern of sexual arousal than were a combined group of offenders against children.”²⁷

Finally, while the reasons behind the abuse may not be clear, some suggest that the desire for new pictures can “lead some consumers to abuse their own, or neighbouring children, in order to supply fresh images for barter or sale.”²⁸

²⁵ Dr. Michael Bourke and Andres Hernandez, “The Butner Study Redux: A Report of the Incidence of Hands-On Child Victimization by Child Pornography Offenders,” (in press), pp. 17–18. There is some ongoing debate about this study.

²⁶ Ibid., p. 18.

²⁷ Dr. Michael Seto et al. “Child Pornography Offenses Are Valid Diagnostic Indicator of Pedophilia,” *Journal of Abnormal Psychology*, 2006 115(3), p. 613.

²⁸ Susan J. Creighton, “Child pornography: Images of the abuse of children,” November 2003. www.nspcc.org.uk.

Younger victims and increasing violence

In addition to their growing number, child sexual abuse images are getting more and more shocking. As Ontario Provincial Police (OPP) Detective Inspector Angie Howe explained to the Senate Legal and Constitutional Affairs Committee, “The images are getting more violent and the children in the photos are getting younger. As recently as one year ago, we did not often see pictures with babies, where now it is normal to see babies in many collections that we find. There is even a highly sought after series on the Internet of a newborn baby being violated. She still has her umbilical cord attached, she is that young.”²⁹

“Daddy, it hurts. It hurts so bad.”

—Audiotape of a young girl as her father abuses her

“Many of the images which I see on a regular basis show severe vaginal and anal assault against toddlers, bondage of these children with gags in their mouths, ligatures around their necks, and on occasion, physical beatings in conjunction with video clips of brutal oral, vaginal and anal penetration.”³⁰

—Dr. Sharon Cooper, Speech to U.S. Congress in 2006

- Younger children:
 - ▶ 83 percent of children are 12 years old or younger.³¹
 - ▶ 39 percent had images of children between the ages of 3 and 5.³²
 - ▶ 19 percent had images of infants under 3 years old.³³
- More violent content:
 - ▶ Over 80 percent of the images involve penetration.³⁴
 - ▶ Over 70 percent show sexual contact between a minor and an adult.³⁵
 - ▶ 20 percent of the images involve torture or bondage.³⁶
 - ▶ The number of images of “serious child abuse” has quadrupled between 2003 and 2007.³⁷
 - ▶ 87 percent had images of prepubescent children that were highly graphic.³⁸

²⁹ OPP Detective Inspector Angie Howe, Senate Legal and Constitutional Affairs Committee, 2005.

³⁰ Dr. Sharon Cooper, Opening Oral Testimony for the US Senate Committee on Commerce, Science and Transportation, September 19, 2006.

³¹ H.R. 4120, *An Act to amend title 18, United States Code, to provide for more effective prosecution of cases involving child pornography, and for other purposes.*

³² *National Juvenile Online Victimization Study* (NJOV) 2004.

³³ Ibid.

³⁴ Janis Wolak et al. “Internet Sex Crimes Against Minors: The Response of Law Enforcement,” November 2003.

www.missingkids.com/en_US/publications/NC132.pdf.

³⁵ Ibid.

³⁶ CTV.ca, July 23, 2006.

³⁷ According to Internet Watch Foundation; Jonah Rimer, *Literature Review—Responding to Child & Youth Victims of Sexual Exploitation on the Internet*, 2007, p. 16.


³⁸ *Juvenile Online Victimization Incidence Study* (JOVIS) 2004.



Examples of this violence are being seen across Canada. In an Ontario case, a father pled guilty to possessing and accessing child sexual abuse images, which included a five-minute video in which a naked 9-year-old girl is anally, vaginally and orally penetrated and another in which an adult male attempts to penetrate a 6-year-old girl. Police in Winnipeg arrested an American man who had videos of girls between the ages of 4 and 12 performing

oral sex on adult men. In Quebec, provincial police arrested several men alleged to be involved in an international child pornography ring that operated over the Internet. The victims of this ring included those of elementary school age and a baby who was just a few months old.³⁹ Sadly, these examples are not even the worst of the material available.

³⁹ Peter Rakobowchuk, "Quebec police say baby was part of porn ring," *The Toronto Star*, June 25, 2008.



"Sometimes, you can hear
the children cry."

—Paul Gillespie, retired Detective Sergeant, Toronto Police Sex Crime Unit

Progress to Date

CANADA'S CURRENT CHILD PORNOGRAPHY LEGISLATION was passed in 1993 and then updated in 2002 to respond to the new reality of the Internet. The update included the creation of the new offence of using the Internet to communicate with a young person for the purpose of facilitating the commission of a sexual offence against that child—commonly known as “child luring.”

Two years later, the federal government launched the National Strategy to Protect Children from Sexual Exploitation on the Internet. The strategy included the creation of the Royal Canadian Mounted Police (RCMP) National Child Exploitation Coordination Centre, a

clearing house and coordination centre for international requests to conduct investigations in Canada related to child sexual exploitation on the Internet. On February 10, 2009, the Minister of Public Safety announced the renewal of this strategy.

In 2005, Parliament expanded the definition of child pornography, increased the maximum penalty for all child pornography offences and introduced mandatory minimum penalties. That same year, the Manitoba-based organization Cybertip.ca became Canada's national tipline for reporting the online sexual exploitation of children.⁴⁰

⁴⁰ www.protectchildren.ca/app/en/.

During this period, Canada took action not just at home, but in the international community, leading our counterparts in learning how to better respond to the abuse of children.

Canada sponsored the United Nations Guidelines on *Justice Matters involving Child Victims and Witnesses of Crime*.⁴¹ Canada was also a signatory to the United Nations *Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution, and child pornography* (2000), which requires state parties to protect children from all forms of sexual exploitation and abuse and to take appropriate measures to prevent the exploitative use of children in pornographic performances and materials.

In 2007, Canada's Ministers of Justice and Public Safety joined other G8 Ministers and agreed to accelerate efforts "to ensuring the implementation and effectiveness of our own laws relating to child pornography, and to taking steps to update and improve those laws when necessary and where appropriate."⁴² That same year, the Federal/Provincial/Territorial (FPT) Ministers responsible for Justice "expressed serious concern about child pornography on the Internet and asked officials, on a priority basis, to complete their work in examining measures, including legislation, to increase cooperation of Internet Service Providers in assisting law enforcement officials to identify criminals and rescue child victims."⁴³

In 2007, the federal government also took further steps to protect children by raising the age of consent from 14 to 16, enhancing the dangerous offender provisions of the *Criminal Code* and dedicating an additional \$6 million to the RCMP to protect children "from online sexual exploitation..."⁴⁴

In January 2008, former Public Safety Minister Stockwell Day gave \$2 million to the Canadian Centre for Child Protection, which operates Cybertip.ca, declaring it as "another concrete action that our government is taking to protect children from online adult sexual predators, and to prevent them from being sexually abused."⁴⁵

In September 2008, the FPT Ministers responsible for Justice agreed that "Canada's response to child pornography could be enhanced by federal legislation requiring any agency whose services could be used to facilitate the commission of online child pornography offences to report suspected material."⁴⁶ This would bring Canada in line with other countries, like the United States and Australia which, under federal law, require Electronic Service Providers (ESPs) to report the discovery of child sexual abuse images. Some provinces, like Manitoba and Ontario, have passed legislation regarding mandatory reporting of child sexual abuse images.

⁴¹ Part of the International Labour Organization's *Convention Concerning the Prohibition and Immediate Action for the Elimination of the Worst Forms of Child Labour*, *Convention 182*.

⁴² G8 Justice and Home Affairs Ministers, May 24, 2007. www.g8.gc.ca/childpornography-en.asp.

⁴³ Federal-Provincial-Territorial Meeting of Ministers responsible for Justice Meet [news release], Winnipeg, Manitoba, November 14–16, 2007. www.scics.gc.ca/cinfo07/830926004_e.html.

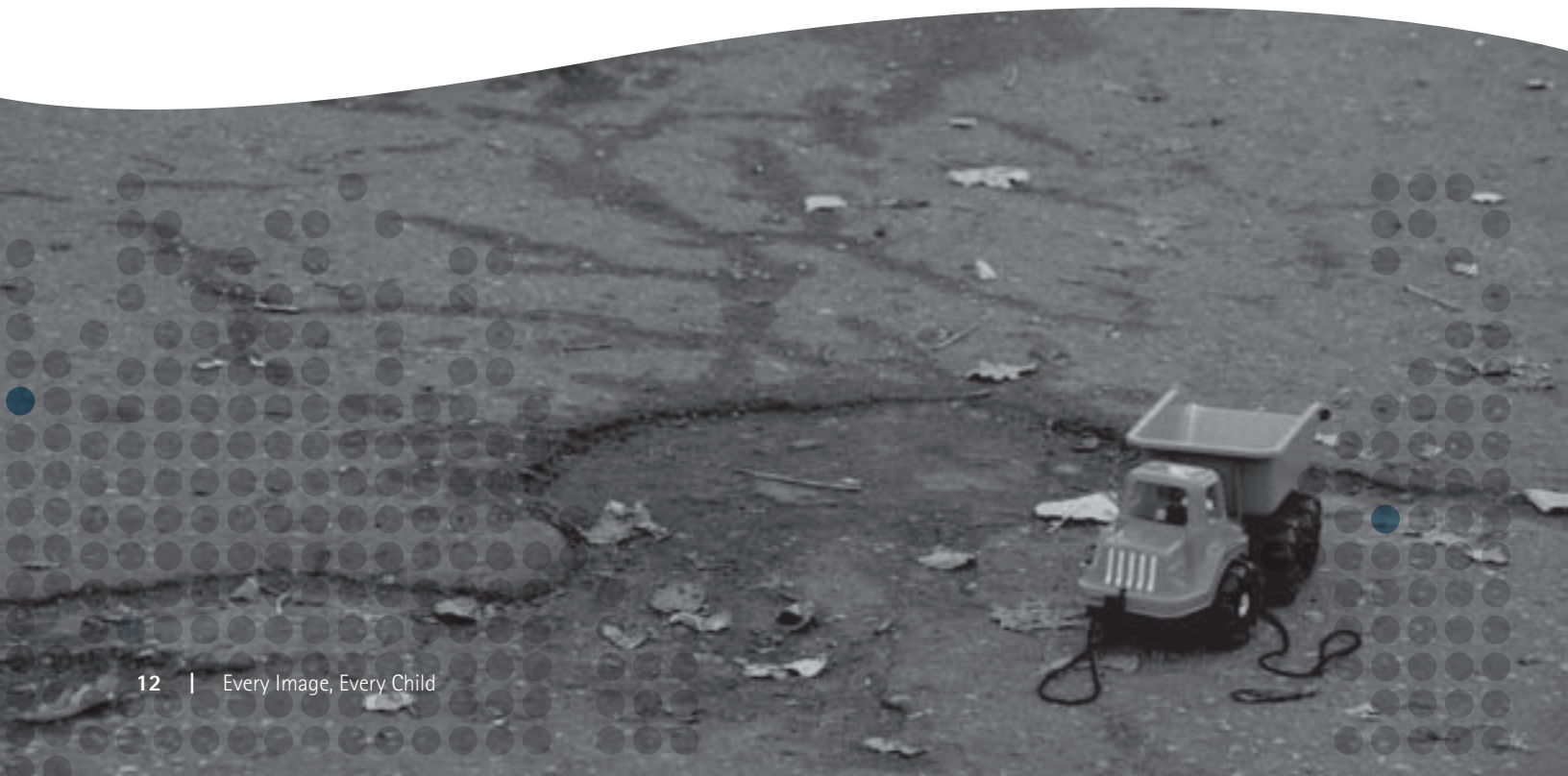
⁴⁴ The Honourable Jim Flaherty, 2007 Budget Speech, March 19, 2007. <http://www.budget.gc.ca/2007/speech-discours/speech-discours-eng.html>.

⁴⁵ www.publicsafety.gc.ca/media/nr/2008/nr20080129-eng.aspx.

⁴⁶ September 5, 2008. http://canada.justice.gc.ca/eng/news-nouv/nr-cp/2008/doc_32302.html.

We encourage the Government to proceed with legislation that would require not only ISPs, but social networking sites, computer repair shops and Internet content hosts to report suspected child pornography. However, this must be part of an overall government strategy to combat this problem. Mandatory reporting on its own is not likely to make a significant difference in the fight against online child sexual exploitation. Law enforcement agencies

report now that they are struggling to keep up with the number of cases they have. The most serious problem is not lack of reports, but about accessing information about suspects, identifying children and preventing future abuse. The federal government must avoid acting on mandatory reporting just to be seen to be doing something without addressing the priority issues identified in this report.





"It made no difference to me whether the abuser was under the covers or behind the lens or behind the computer. I was there because they wanted to be amused by the corruption and degradation of me."

—Shy Keenan, former victim and a children's rights advocate

What More Needs to Be Done— Recommendations

DESPITE ITS PAST SUCCESSES, CANADA HAS MUCH MORE TO DO.

There are a number of sizable gaps where children are falling through the cracks and offenders are gaining momentum. We must move to address these gaps now, before we fall too far behind.

Specifically, we must be honest about the horror of the situation and address it as such. We need to reconsider which has higher value: an offender's right to anonymity or the real harm being done to children. We need to give

authorities the tools they need to identify these children and rescue them and then, once the victims are found, we need to have the resources and expertise in place to properly care for these children and to help them heal. Finally, 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.

While the issue is enormous, this report presents nine practical and feasible recommendations to address the issue of child sexual exploitation as it pertains to the Internet.

1. CHILD PORNOGRAPHY— A DANGEROUS TERM

To begin, it is important to first address the term “child pornography.”

In 2007, in a special report entitled *Reinforcing the International Fight Against Child Pornography*, the G8 Justice and Home Affairs Ministers noted that while the term “child pornography” is used commonly in legislation and international conventions, it “does not appropriately or adequately describe the severe abuse and exploitation of children that is involved in these visual representations.”⁴⁷

As the Ministers point out, the real nature of the problem is, in essence, sexually explicit images or representations of children. The term “pornography,” however, is commonly understood to be associated with depictions of sexual activity between *consenting* individuals. 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 real harm that is experienced by young victims and the seriousness of the activities of those persons who sexually exploit children in this way. “This misunderstanding compromises the effectiveness of our very important efforts to protect children from this form of sexual exploitation.”⁴⁸

This applies to other similar terms, such as “kiddie porn” or “child porn,” which may also contribute to the public misperception about what law enforcement is finding on the Internet. As Jim Gamble, Chief of the Child Exploitation and Online Protection Centre, points out, “If a woman is raped and her attacker makes a video of it, no one would dare suggest the video was adult pornography. He is a rapist, not a pornographer.”⁴⁹

For this reason, this report uses the term “child sexual abuse images.” We will use the term “child pornography” only when making specific reference to the *Criminal Code of Canada* or the laws of other countries, as there is no internationally agreed-upon term at this time.⁵⁰ While no words can adequately convey the horror these children are suffering, we believe the term “child sexual abuse images” (or videos) more accurately describes that harsh reality than “child pornography.” Based on this, we recommend that legislation be amended to better distinguish child sexual abuse images from the adult, legally based commercial industry.

RECOMMENDATION 1—That the federal government introduce legislation to amend the child pornography provisions in the *Criminal Code* to provide a more accurate description of the crime (i.e. such as child sexual abuse images, child sexual abuse videos, child sexual abuse writings) to ensure a more accurate reflection of the harm that is done to victims.

⁴⁷ www.virtualglobaltaskforce.com/news/G8Statement.pdf.

⁴⁸ www.canadainternational.gc.ca/g8/ministerials-ministerielles/2007/child_porno-enfant_porno.aspx?lang=eng.

⁴⁹ The U.K. created the Child Exploitation and Online Protection (CEOP) Centre to play a decisive role in partnership with the Department for Children, Schools and Families (DCSF), police forces, offender managers, children’s services and other stakeholders in the protection of children, young people, families and society from pedophiles and sex offenders—particularly those who use the Internet. The CEOP Centre works across the U.K. and uses international links to combine police powers with the expertise of children’s charities, business sectors, government and other interested organizations all focused on tackling child sex abuse wherever it happens.

⁵⁰ In Queensland, the term used is “child exploitation material.” CRIMINAL CODE 1899 - SECT 207A.

2. RESCUING CHILDREN FROM INTERNET-FACILITATED SEXUAL ABUSE

The key step in rescuing victims of abuse is to identify and locate them. While this may seem a daunting task, ironically the same Internet technology that facilitates the repeated victimization of children can help law enforcement identify and rescue those same victims.

One of the most powerful clues that police have available to assist them in this regard is the Internet Protocol or “IP” address.

An IP address is a numerical identifier given to a particular computer or device when it is hooked up to the Internet—something like a licence plate for a car. When offenders are exchanging images, the IP address is often publicly accessible. This information can often help authorities to determine the location of the offender by providing more information about the Internet Service Provider (ISP) the offender is using (i.e. the company that is providing the abuser with Internet access) as well as the geographic region of the user.

In some cases, the IP address can actually narrow down the location of the abuser to a specific city. Once a geographic area is defined, the next step is to contact the ISP and to ask for the name and address of the customer registered to that IP address.

Unfortunately in Canada, this is where authorities sometimes hit a dead end and the investigation is forced to shut down. According to the *Personal Information Protection and Electronic Documents Act* (PIPEDA), ISPs in Canada “may,” but are not legally obliged to, provide police with information such as the name and address of customers who are known to be exchanging or distributing child sexual abuse images.

Currently, police send a standard letter to the ISP, which asks for customer name and address information for a specific IP address and for a specific date and time.⁵¹ Whether or not the ISP provides this information is up to the individual company. Many ISPs have provisions in their service agreement that say they will disclose *any information* they, in their sole discretion, deem necessary to satisfy any applicable law, regulation, legal process, or government request.⁵² The *Bell Code of Fair Information Practices* defines “personal information” for a customer as “a customer’s credit information, billing records, service and equipment, and any recorded complaints.”⁵³ Basic subscriber information such as the customer’s name and address is *not* considered personal information for the purposes of the Privacy Policy.

Even though many ISPs do cooperate, 30 to 40 percent of requests are still denied.⁵⁴ Some ISPs are hesitant to cooperate for fear of resulting legal action by customers, whereas others even go so far as to advertise their lack of cooperation with police to attract customers.⁵⁵

When it comes to protecting our children, depending on the goodwill of any industry is not good enough.

⁵¹ The letter was developed by the Canadian Coalition Against Child Exploitation (CCAICE), a voluntary group of partners that work to reduce child sexual exploitation on the Internet. CCAICE includes industry, government, non-governmental and law enforcement stakeholders from across the country. The existing arrangement is based on paragraph 7(3)(c) of the *Personal Information Protection and Electronic Documents Act*.

⁵² *Bell Customer Service Agreement*, p. 14.

⁵³ *Bell Code of Fair Information Practices*, Definitions, p. 4.

⁵⁴ NCECC Submission to Public Safety Canada, “Customer Name and Address Information Consultation,” October 2007.

⁵⁵ *Ibid.*, p. 4.



Giving authorities the tools they need

The idea of requiring ISPs to provide customer name and address information is not new. For years, the law enforcement community has been calling for legislative reforms to require ISPs to provide this information without judicial authorization (i.e. a warrant).⁵⁶

The same sentiments were expressed in 2007 when the Office of the Federal Ombudsman for Victims of Crime brought together law enforcement experts from across Canada for a roundtable on Internet-facilitated child sexual abuse. Without exception, the number one barrier to pursuing cases identified by law enforcement attending the roundtable was the lack of access to customer name and address information.

The RCMP's National Child Exploitation Coordination Centre (NCECC) warns, "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 online child exploitation matters, *the result is that many investigations cannot proceed* (emphasis added)."⁵⁷

A 2007 Department of Public Safety consultation document on customer name and address information provided a similar warning: "If the custodian of the information is not cooperative when a request for such information is made, law enforcement agencies may have no means to compel the production of information pertaining to the customer.... *The availability of such building-block information is often the difference between the start and finish of an investigation* (emphasis added)."⁵⁸

Sadly, this challenge translates into unsuccessful rescue efforts. In one case, an online undercover officer investigating the live online sexual abuse of a child on a Friday evening requested the customer name and

⁵⁶ A recent report prepared by Deloitte for the Canadian Association of Police Boards, entitled *Report on Cybercrime in Canada* (April 25, 2008, pp. 1–2), which included interviews with law enforcement, Crowns and others with experience in this area, said there was support for changes to existing legislation that would enable information sharing with law enforcement agencies, with lower judicial standards than those now applied to search and seizure warrant and mandatory reporting requirements for child pornography.

⁵⁷ NCECC Submission to Public Safety Canada, "Customer Name and Address Information Consultation," October 2007.

⁵⁸ www.publicsafety.gc.ca/prg/ns/cna-en.asp. The document also clarified "the possible scope of CNA information to be obtained is later identified, but *it should be noted from the outset that it would not, in any formulation, include the content of communications or the Web sites an individual visited while online...*"

address information from the ISP but was told to call back on Monday during regular business hours.⁵⁹ In June 2007, a law enforcement agency asked an ISP for customer information because it had reason to believe children were at risk. The ISP refused to provide the information unless the investigator produced judicial authorization. It was not until pressure was applied by Child Welfare Services that the ISP finally provided the customer's name. By this time, the suspect had moved and dismantled his computer.

In a few cases, police have been able to convince ISPs of the importance of the information by going to extreme lengths. Such was the case when an officer investigating live sexual abuse was told by the ISP to get judicial authorization. The ISP became cooperative only after the officer held the phone to the computer speakers to let the representative hear the child's screams.

The right to privacy

"We recognize that privacy is an important value underlying the right to be free from unreasonable search and seizure and the right to liberty. However, the privacy of those who possess child pornography is not the only interest at stake in this appeal. The privacy interests of those children...are engaged by the fact that a permanent record of their sexual exploitation is produced."

—Madam Justice L'Heureux-Dubé⁶⁰

Any public policy debate that involves the Internet must include the issue of privacy and the very real and legitimate privacy concerns that Canadians have.

The public is rightly concerned about their privacy and has a right to be protected from unreasonable search and seizure. As such, privacy should be considered when deciding what kinds of information law enforcement should have access to regarding Internet customers. Efforts to address enforcement issues to date, however, have been too narrowly focused on false warnings of "Big Brother" or have fostered misconceptions about what kind of information police are able to obtain with an IP address and a customer's name and address. Very little attention has been given to the real, and more serious, privacy interests of the children whose images of abuse and torture are being traded.

Unfortunately, Canadians have been misled about the potential privacy implications of legislation that would permit law enforcement access to customer name and address (CNA) information. For example, one privacy advocate contends, "CNA information, like name and address, are keys to acquiring other personal information, including highly sensitive data such as health or financial records."⁶¹ The author goes on to argue that "...the government is in fact seeking enhanced search powers through expedited processes and lower standards, thereby slashing privacy safeguards and expectations."⁶² Another said, in response to an Ontario Superior Court decision that upheld police access to CNA information without a warrant,⁶³ "It is not just your name. It is your whole Internet surfing history."⁶⁴

⁵⁹ Ibid., p. 5.

⁶⁰ *R. v. Sharpe*, 2001 SCC 2, [2001] 1 S.C.R. 45, para. 189.

⁶¹ Ian Kerr, Submission to the Customer Name and Address Consultation, October 19, 2007. www.idtrail.org/content/view/full/763/42/.

⁶² Ibid.

⁶³ *R. v. Wilson*, ONCJ St-Thomas, no. 4191/08, February 10, 2009.

⁶⁴ Shannon Kari, "Judge's ruling could let police access IP data without warrant," *Ottawa Citizen*, February 13, 2009.

These points touch on the two most common arguments put forward by privacy advocates:

1. It is inappropriate for law enforcement to seek, without judicial authority, the name and address of a potential offender.
2. Providing customer and name and address information gives police enhanced powers to review and collect more personal information, such as health records or a client's Internet surfing history.

These points are false and confuse the issue by offering dangerous misconceptions. First, a person's name and address are not private and law enforcement does not need judicial authorization to obtain them. Second, if police want more information about a suspect, such as his or her Internet surfing history or medical records, they must obtain judicial authorization.

In *R. v. Plant*, the Supreme Court of Canada said that for information to be constitutionally protected, it must be at the "biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state, and that the information must disclose 'intimate details' about the 'personal lifestyle or private decisions.'"⁶⁵

The *Plant* case involved a police investigation into a marijuana grow-op. The police obtained information from the electricity company—another service provider—regarding the owner's electricity use. They used this information to obtain a search warrant. The Supreme Court said:

"The police check of computerized records was not unreasonable.... In view of the nature of the information, the relationship between the accused and the electrical utility, the place and manner of the search and the seriousness of the offence under investigation, it cannot be concluded that the accused held a reasonable expectation of privacy in relation to the computerized electricity records which outweighed the state interest in enforcing the laws relating to narcotics offences. While they reveal the pattern of electricity consumption in the residence, the records do not reveal intimate details of the accused's life. Since the search does not fall within the parameters of s. 8 of the *Charter*, this information was available to the police to support the application for a search warrant."⁶⁶

In *R. v. David Ward*, Justice Lalonde said, "There is certainly no evidence...that disclosure of the applicant's name and address only, absent the police obtaining a search warrant, would open the floodgates to intimate personal details about the applicant's lifestyle, habits and choices."⁶⁷

⁶⁵ *R. v. Plant*, [1993] 3 S.C.R. 281.

⁶⁶ *Ibid.*

⁶⁷ *R. v. David Ward*, Sudbury Court File No. 071751, June 16 and 17, 2008.



In February 2009, Justice Lynne Leitch of the Ontario Superior Court ruled “[t]here is no reasonable expectation of privacy in the information provided by Bell considering the nature of that information. One’s name and address... are not biographical information one expects would be kept private from the state. It is information available in a public directory....”⁶⁸ This marked the first time a Superior Court had issued such a ruling, although some lower courts have made consistent rulings.⁶⁹

In *R. v. Quinn*, at the request of law enforcement, a bank confirmed that a specific account belonged to the appellant. This information was later used to obtain a search warrant.⁷⁰ The British Columbia Court of Appeal upheld the warrant and finding saying, “[T]here was no search, much less any unreasonable search as envisioned in the Charter.”⁷¹

Obtaining a suspect's name and address is already common practice during an investigation. Police get access to an individual's name and address in a variety of ways. If they pull your car over, you must show them your licence. If you are seen driving away from an accident, they can access your information through your licence plate.

⁶⁸ *R. v. Wilson*, ONCJ St-Thomas, no. 4191/08, February 10, 2009.

⁶⁹ *Ibid.* Most decisions support the principles that a customer's name and address are not “private” information, but there have been dissenting opinions (*R. v. Kwok*).

⁷⁰ *R. v. Quinn* 2006 BCCA 255.

⁷¹ *Ibid.*, para. 93.

The federal government already authorizes agencies the power to collect this type of information without a warrant. For example, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), which works to identify money laundering and terrorist activities financing, can request information such as business records, and enter business premises, without a warrant.⁷² The information must be kept in such a way as to enable FINTRAC access in a timely fashion and failure to comply with these requirements could lead to imprisonment for up to five years.

Certain ISPs will only provide CNA information without a warrant in cases where “imminent” danger is identified. Some ISPs have agreed to provide the information upon request only if someone is in imminent danger. However, if police cannot prove imminent danger the ISPs will usually require judicial authorization.⁷³

This is problematic for a number of reasons, including the fact that imminent danger is not always obvious. In 2006, police in Aylmer, Quebec, arrested a 19-year-old man after he sent child sexual abuse images to an undercover Ottawa police officer online. After the arrest, the man admitted to sexually abusing his 8-month-old son and filming it. At the time of his arrest, the police had no idea he was abusing his son.⁷⁴ In this scenario, because police could not have known or demonstrated in advance that a child was in imminent danger, a little boy would have gone on being abused. Similarly, in February 2009, law enforcement in Ontario arrested over 30 men during a province-wide child pornography sweep. A 12-year-old girl was removed from the home of one of the men arrested on suspicion of distributing child sexual

abuse images, but at the time of his arrest, law enforcement had no reason to believe the man was abusing a child. Clearly, it is not possible for ISPs to determine the level of risk to a child in these situations.

If imminent danger cannot be proven and law enforcement is required to get a warrant, there is a greater risk to the child. First, warrants take time and law enforcement may not be able to get one in time to rescue the child in danger. The more time police spend trying to get judicial authorization for information that is not personal or private, the less time they have available to identify and rescue children. As stated by the Public Safety Minister, “In some of these cases, time is of the essence. If you find a situation where a child is being exploited live online at that time...police services have had good cooperation with a lot of internet service providers, but there are some that aren’t so cooperative.”⁷⁵

Second, a warrant cannot be obtained in the investigation of a criminal offence until sufficient information “to support reasonable and probable grounds for that offence exists.”⁷⁶ Obtaining basic CNA information is part of the information that would assist in obtaining a warrant.

Privacy rights of the victim

A balanced discussion of privacy must also consider the rights of the victim.

For victims whose abuse has been shared on the Internet, there is no privacy. They must grow up knowing these images or videos will be on the Internet for the rest of their life. It is a privacy violation that never ends.

⁷² FINTRAC gets its authority from the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.

⁷³ CBC News, “Search warrants for child porn too slow, say RCMP,” April 2, 2008. www.cbc.ca/canada/prine-edward-island/story/2008/04/02/childporn-warrants.html.

⁷⁴ CBCNews.ca, “Quebec man jailed for molesting infant son, making child porn,” July 20, 2007.

⁷⁵ Bill Curry, “New law to give police access to online exchanges,” *The Globe and Mail*, February 12, 2009.

⁷⁶ NCECC Submission to Public Safety, “Customer Name and Address Information Consultation,” October 2007, p. 7.

Privacy rights are established in the *Canadian Charter of Rights and Freedoms* and international forums. For example, section 7 of the Charter guarantees the right to life, liberty and security of the person, which is certainly undermined by child pornography.⁷⁷ Privacy is also one of the principles the federal government is required to consider under the *Canadian Statement of Basic Principles of Justice for Victims of Crime*. The United Nations Resolution on Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime also affirms that children have a right to privacy and it should be protected as a matter of primary importance.

In the case of child sexual abuse images, the invasion of privacy goes far beyond simply sharing personal information. Madam Justice L'Heureux-Dubé wrote, "If disseminated, child pornography involving real people immediately violates the privacy rights of those depicted, causing them additional humiliation."⁷⁸ She went on to say, "The law intrudes into the private sphere because doing so is necessary to achieve its salutary objectives. The privacy interest restricted by the law is closely related to the specific harmful effects of child pornography. Moreover, the

provision's beneficial effects in protecting the privacy interests of children are proportional to the detrimental effects on the privacy of those who possess child pornography."⁷⁹

Two recent decisions have caused some concern about the willingness of the court to consider the privacy interests of the child victim.

The first case involved an artist (Katigbak) who had over 500 images and 30 video clips that constituted child pornography. He claimed he was working on an artistic project (over a six-year period of time) to raise awareness of the effect of child pornography or sexual abuse on the children.⁸⁰ The other case (Sauve) involved a manager of a group home where some clients had pedophilic tendencies; he claimed he collected images to help treat a client.⁸¹

Both men were acquitted because the Courts accepted the accused's justifications for possessing and collecting the images. Both cases addressed the issue of "undue harm to the child" and found that the actions of neither man put children under the age of 18 at undue risk. In Katigbak, the Court relied on the fact that the accused did not purchase the images, he was not sexually motivated and did not intend to distribute them. The Court said this "negatives the concern that the victims are being re-victimized by a viewing of the images."⁸² In Sauve, the Court said Parliament was not referring to a general risk of harm to children.

Neither Court, nor the two accused, considered the harm done to the children whose images were being collected. No matter the reason behind it, these children gave no permission to either man to access or collect their images. In doing so, these men contributed to the victims' ongoing abuse.



⁷⁷ *R. v. Sharpe*, 2001 SCC 2, [2001] 1 S.C.R. 45, para. 189.

⁷⁸ *Ibid.*, para. 135.

⁷⁹ *Ibid.*, para. 240.

⁸⁰ *R. v. Katigbak* (2008) Reasons for Decision. Some of the alleged offences were committed before the 2005 amendment and prior to that the *Criminal Code* referred to "artistic merit or an educational, scientific or medical purpose."

⁸¹ *R. v. Sauve* (2008) O.J. No. 4230.

⁸² *R. v. Katigbak* (2008) Reasons for Decision, para. 36.

The Crown is appealing the Katigbak decision. We urge the Department of Justice to monitor these cases to determine if an amendment is necessary to highlight the privacy interests of the children whose images are being collected.

As a final point, it is important to consider the following: The more time police spend trying to get judicial authorization for information that is not personal or private, the less time they have available to identify and rescue children.

The need for legislative change

The RCMP's NCECC says "the single most important challenge facing investigators of Internet facilitated child exploitation ahead of all other issues, has been their inability to obtain basic customer information such as someone's name and address from Internet Service Providers (ISPs)."⁸³

This was confirmed in 2007 when our office held a roundtable with law enforcement from across the country. At the roundtable, law enforcement identified its inability to acquire customer name and address information as the single biggest obstacle to identifying offenders and rescuing child victims of Internet-facilitated child sexual abuse.

In 2006, the Standing Committee on Access to Information, Privacy and Ethics conducted a review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). It heard from victims' groups and law enforcement that, although PIPEDA authorizes ISPs to provide basic information to law enforcement, many were not doing so. Clayton Pecknold of the Canadian Association of Chiefs of Police explained the challenges the police face:

"...we are increasingly seeing some companies interpreting lawful authority to mean that a warrant or court order is required before they comply. This is an interpretation that is not, in our respectful view, consistent with the intent of the drafting of the act. Such an interpretation by companies, while no doubt grounded in a legitimate desire to protect their customers' privacy, is overly restrictive and defeats, in our view, the intent of paragraph 7(3)(c.1)."⁸⁴

In 2007, the Committee released its fourth report and recommended:

"...that consideration be given to clarifying what is meant by "lawful authority" in section 7(3)(c.1) of PIPEDA and that the opening paragraph of section 7(3) be amended to read as follows: 'For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization **shall** disclose personal information without the knowledge or consent of the individual but only if the disclosure is [...].'"

⁸³ NCECC Submission to Public Safety Canada, "Customer Name and Address Information Consultation," October 2007, p. 1.

⁸⁴ Standing Committee on Access to Information, Privacy and Ethics, Meeting 30, February 13, 2007. www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=2695445&Language=E&Mode=1&Parl=39&Ses=1.

Responding to the report, the former Minister of Industry confirmed “that the purpose of s.7(3)(c.1) is to allow organizations to collaborate with law enforcement and national security agencies without a subpoena, warrant or court order. Organizations who share information with government institutions, including law enforcement and national security agencies, in accordance with the requirements of this provision, are doing so in compliance with PIPEDA.”⁸⁵

In October 2007, the Department of Industry released a consultation document on several issues relating to the committee’s report, including the proposal to clarify lawful authority. The Office of the Federal Ombudsman for Victims of Crime submitted a written brief to the Minister calling upon him to enact legislation quickly to clarify lawful authority as well as to make a further amendment to the legislation to require ISPs to provide CNA information to police investigating child sexual abuse cases.⁸⁶

In a response sent in November 2007 to the Ombudsman’s office, the former Minister of Industry said, “The Government of Canada accords the highest importance to the safety and security of Canadians and recognizes the particularly vulnerable nature of children in the online environment.” The former Minister acknowledged that the current law has created “challenges for law enforcement investigations” and that law enforcement reports that its ability to gain access to “basic information that is essential and often quite urgent” has been hindered. He stated that PIPEDA was not intended to be an impediment to the cooperation between companies and law enforcement, yet he said, “Obligations to collaborate in investigations and the establishment of consequences for obstruction currently

rest with the *Criminal Code of Canada*. As such, a requirement for compulsory disclosures or information would be incompatible with the purpose of PIPEDA....”⁸⁷

Canada has fallen behind on this point. Other countries, including the U.K., Australia and the U.S., have passed legislation that does not require law enforcement to secure judicial authorization before accessing CNA from an ISP.⁸⁸

In the fall of 2007, the Department of Public Safety released its own consultation document on customer name and address information. The Office of the Federal Ombudsman for Victims of Crime participated in the consultation, urging the former Minister of Public Safety to introduce legislation that would require ISPs to provide CNA information to law enforcement. In response, the Government said it was examining how best to address this serious issue, including the possibility of legislation in this area.⁸⁹ On February 11, 2009, the current Minister of Public Safety confirmed he was considering legislation to address problems of enforcing laws in the age of the Internet. Specifically, the Minister stated, “If somebody’s engaging in illegal activities on the Internet, whether it be exploitation of children, distributing illegal child pornography, conducting some kind of fraud, simple things like getting username and address should be fairly standard, simple practice. We need to provide police with tools to be able to get that information so that they can carry out these investigations.”⁹⁰

RECOMMENDATION 2—That the federal government expedite legislation to require ISPs to provide customer name and address information to law enforcement.

⁸⁵ Government Response to the Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics, Statutory Review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). www.ic.gc.ca/eic/site/ic1.nsf/eng/h_02861.html.

⁸⁶ www.victimfirst.gc.ca.

⁸⁷ Letter from the Honourable Jim Prentice, Minister of Industry, November 29, 2007.

⁸⁸ The scheme set out in Bill C-74 and the department’s consultation appear to be more restrictive than that of the other three countries. Dominique Valiquet, *Telecommunications and Lawful Access: II. The Legislative Situation in the United States, the United Kingdom and Australia*, February 28, 2006, Library of Parliament. www.parl.gc.ca/information/library/PRBpubs/prb0566-e.html.

⁸⁹ “Government Response to the Annual Report of the Federal Ombudsman for Victims of Crime, April 2007 to March 2008.” http://canada.justice.gc.ca/eng/news-nouv/nr-cp/2009/doc_32330.html.

⁹⁰ Bill Curry, “New law to give police access to online exchanges,” *The Globe and Mail*, February 12, 2009.



3. GATHERING EVIDENCE— DISAPPEARING INFORMATION

As discussed, the ability of police to identify and rescue children in an expedient manner is tied directly to their ability to get information about Internet customers. Obtaining this information, however, is not always straightforward, even with the cooperation of ISPs because in some cases they have already purged it from their systems.

“Client logs” contain information about when a client logged onto the Internet, what the client did while on the Internet and which IP address the session was linked to. This information is very useful for law enforcement agencies that are investigating a case. Police are required to obtain judicial authorization to obtain this information; however, too often even after police have authorization the information is no longer available because it has been erased or purged.

ISPs are not legally obligated to retain client logs. There is also no standard length of time for data retention. In some cases, data are purged after four hours.⁹¹ If the information no longer exists, the investigation cannot proceed. This obviously has serious implications for victims.

The Kids Internet Safety Alliance (KINSA) has called for legislation that requires ISPs to “retain the IP address logs, indicating which subscriber had a particular IP address, for a period of 5 years.” KINSA also promotes a requirement that ISPs retain subscriber information for past customers for the same time period.⁹²

Data retention requirements would require providers to collect and keep information from all users of a communication service—regardless of whether or not they are the subject of an investigation. This would ensure that information vital to an investigation is not deleted before the police can obtain a search warrant or production order to access the specific data.

⁹¹ NCECC Submission to Public Safety Canada, “Customer Name and Address Information Consultation,” October 2007, p. 5.

⁹² KINSA was incorporated as the Kids’ Internet Safety Association in 2005 and is now known as the Kids’ Internet Safety Alliance. KINSA focuses on advocacy, awareness, training and research. www.KINSA.net.

Other countries have data preservation laws that enable law enforcement authorities, during a criminal investigation, to instruct a service provider to set aside specified data about a specific individual or IP address that is already in the service provider's possession until law enforcement procures the proper documents to require the data's disclosure. Preservation has been the law in the U.S. since April 1996.⁹³

In Canada, ISPs have raised concerns about the cost of data retention, as they have with other aspects of Internet enforcement. While it is beyond the scope of this report to address the issue, the Supreme Court of Canada recently confirmed that police do not have to pay for third parties (in this case, a phone company) to produce records needed in criminal investigations.⁹⁴ The Court heard evidence that the annual cost of TELUS to comply with production order requests would be over \$660,000, which represents 0.023 percent of operating revenue for 2004 and 0.058 percent of Telus' earnings—"...the equivalent of a person earning \$100,000 a year having to spend up to \$58 to comply with jury duty."⁹⁵

Benjamin Perry, assistant law professor at the University of British Columbia, contends, "Internet service providers do make a lot of money off of the sharing of child pornography online" and they "have an obligation to contribute more to eradicate child pornography than they do now."⁹⁶

RECOMMENDATION 3—That the federal government introduce legislation to require ISPs to retain customer name and address data, traffic data and content data for two to five years.

4. ACCESSING AND STORING INFORMATION

Even when authorities are able to obtain customer name and address information, they may still hit roadblocks if they come across offenders who have password-protected or heavily encrypted computer systems.

While authorities obviously make every effort to get the offender to cooperate, there is no provision in current legislation that makes it a crime for offenders to withhold this information. Evidently, offenders are not inclined to give this information willingly, as they know it may lead to evidence and material that could be used against them in a court of law.

Some law enforcement organizations report cases where they have not been able to access a computer because they could not break the encryption. In these cases, there is no other option than to drop the charges. As the technology becomes more sophisticated and online predators become increasingly savvy, police are concerned that more and more people will encrypt their computers.

There are certain provisions in the *Criminal Code of Canada* that address cooperation as required when police suspect someone of driving while under the influence of alcohol. For example, it is a criminal offence to refuse to take a breathalyzer test when police suspect a person of impaired driving. In the same way that police are unable to assess the level of the driver's inebriation, law enforcement cannot evaluate the scope of the problem with child sexual abuse images until they are able to access the location where they are contained.

⁹³ 18 U.S.C. 2703(f) requires an electronic communications service provider to "take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process" upon "the request of a governmental entity."

⁹⁴ *Tele-Mobile Co. v. Ontario*, 2008, SCC 12.

⁹⁵ *Ibid.*, p. 36.

⁹⁶ Canwest News Service, "Internet service providers profit from online child porn, legal expert says," *National Post*, December 1, 2007.

Similarly, provisions could be included to make it a criminal offence not to provide a password to law enforcement in cases of suspected possession of child sexual abuse images. Although the charge of not providing a password could be lesser than the charge and sentence for possessing and/or distributing the images, the offender would still have a criminal record, may be required to register with the National Sex Offender Registry, may be required to submit DNA to the National DNA Database and would have to forfeit his or her computer.

Subsection 153.1(b) of the *Customs Act* makes it an offence to hinder or prevent an officer from conducting his or her duties as authorized by the Act, including searches. This section has been used with respect to individuals who did not want to provide passwords for portable computers. In addition, laptops can be detained (section 101) until they are examined.

The U.K. and Australia already have in place legislation to assist law enforcement to access computers and equipment that are protected by passwords or encryption. In the U.K., legislation allows law enforcement authorities to ask anyone who has protected electronic data (e.g. encrypted) or who has access to the data's encryption keys

to either give the police the data in a readable format, or to give them the encryption key so it can be accessed.⁹⁷ Failure to do so can result in a jail sentence of up to two years (five years if the matter is one of national security). It is also a criminal offence if disclosure is not made in compliance with an order.

In Australia, police can apply to a magistrate for an order requiring a person to provide any information or assistance that is reasonable and necessary to allow the officer to access data held in a computer. A person who fails to comply with the order is liable to six months' imprisonment.⁹⁸

Canada needs to give authorities the ability to access the evidence. If the courts give law enforcement the right to search a computer, we believe it must also provide the power for police to act on this right and to hold the individual accountable.

RECOMMENDATION 4—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.

⁹⁷ Part III of the *Regulation of Investigatory Powers Act 2000*.

⁹⁸ CRIMES ACT 1914 - SECT 3LA. Person with knowledge of a computer or a computer system to assist access, etc. www.austlii.edu.au/au/legis/cth/consol_act/ca191482/s3la.html.

5. IDENTIFYING VICTIMS THROUGH IMAGE ANALYSIS

Traditionally, police have focused on catching offenders, but with the increase in the creation and distribution of child sexual abuse images and the use of new technologies such as the Internet, police services have new tools they can use to find victims, and are starting to focus more resources in this area. This is especially helpful in the area of child sexual abuse, where many victims do not report crimes to police.

The identification of victims is achieved by image analysis—a highly specialized, exacting and time-consuming process that is conducted by individual law enforcement officers who must devote countless hours to deciphering the clues in the pictures. It is, in effect, good “old fashioned” police work, but done with high-tech tools in a digital environment.

Image analysis has resulted in the rescue of hundreds of children worldwide. In 2003, Toronto police began investigating a series of hundreds of images of the same child. Through a tiny wrist band she had on and a one-millimetre blurred photograph of a logo on a uniform, they traced the child to North Carolina. Authorities there identified her and arrested her father, who is now serving a sentence of 100 years.⁹⁹

The same year, Winnipeg police reviewed a 14-minute video that involved the abuse of two young girls and noticed several clues. They heard a radio station’s call letters, saw tattoos on the abuser and noticed a 1996 U.S. election poster. Winnipeg police notified the U.S. Customs

Service International Child Pornography Investigation and Coordination Center, which traced the radio station to Connecticut. Customs had an older video of one of the girls (which meant she had suffered abuse for years) and age-enhanced the photos, which led to the girls’ identification and rescue.¹⁰⁰

More recently, in 2008, Toronto police arrested a former children’s store employee after discovering 30,000 computer child sexual abuse images on his computer. Police were able to identify three of the victims, whose parents were not aware of the alleged abuse before police intervened.¹⁰¹

Image databases

To help coordinate efforts to identify children through image analysis and manage huge volumes of evidence, law enforcement agencies around the world are developing databases of known child sexual abuse images.

INTERPOL, the world’s largest international police organization, created a database called the INTERPOL Child Abuse Image Database (ICAID). ICAID has been endorsed by the G8 and has hundreds of thousands of images which are submitted by member countries, including Canada. The ICAID uses image recognition software to compare details of where the abuse took place, to connect images from the same series of abuse, or to identify images taken in the same location with different victims. Once a country of origin can be established, the images are sent to police in the countries concerned for follow-up. Investigators have been able to identify and rescue several hundred victims using this system.¹⁰²

⁹⁹ Associated Press, “Child pornographer jailed for 100 years,” *Montreal Gazette*, October 21, 2006.

¹⁰⁰ Jason van Rassel, “Manitoba police making headway,” *Calgary Herald*, June 13, 2006.

¹⁰¹ Michele Henry, “Police find Toronto child porn victims—Man, 36, charged after 30,000 images seized,” *Toronto Star*, October 17, 2008.

¹⁰² INTERPOL Fact Sheet on Crimes Against Children. www.INTERPOL.int.

By sharing images, law enforcement across the country and around the world have a chance to speed up rescue efforts. In one case, images found in Germany were placed in an international INTERPOL database. A Canadian law enforcement officer noticed a cap from a school in New Brunswick, which eventually led to the identification of victims. Without the database, this identification may never have occurred or it might have taken months.

Another way these databases help is by providing information on those victims who have already been identified and rescued, even if their images continue to circulate and be shared. Marking these images with this information could save other law enforcement agencies countless hours and resources, which are better spent on looking for children who are still being abused.

The U.S. has incorporated the building of these databases directly into its investigative process. Law enforcement agencies are required to send all images to the National Center for Missing and Exploited Children (NCMEC). NCMEC's Child Victim Identification Program, created in 2003, serves as the national clearinghouse for child pornography cases across the country and is the main point of contact for international agencies.¹⁰³ Its analysts work to identify victims and individuals who sell, trade and distribute the images. To date, NCMEC has processed at least 15 million images and videos and has helped identify over 1,600 children. In one case, a series of images involving one young girl was tracked to over 13,000 individual investigations in the U.S. alone.

In the U.K., the Child Exploitation and Online Protection Centre (CEOP) has also created an image database, which has directly contributed to the rescue of more than 18 children.¹⁰⁴

Canada is also making strides to create a similar database. The RCMP's National Child Exploitation Coordination Centre (NCECC) is the clearinghouse and coordination centre for international requests to conduct investigations in Canada related to child sexual exploitation on the Internet. NCECC is working to have a database operational shortly. Ultimately, the success of the database will depend on law enforcement agencies forwarding all images to the NCECC.¹⁰⁵

Building expertise

Since image databases cannot automatically identify the children in the images, it is important that both the time-consuming and specialized work of image analysis as well as the development of databases and information-sharing tools be well supported.

The Ontario coordinated provincial strategy, led by the Ontario Provincial Police, includes victim identification/background analysis teams that analyze child abuse images for clues of the children's whereabouts. The integrated model coordinates the increased identification, provides support services to child victims (and their families) of Internet sexual abuse and exploitation, and assists in preventing the cycle of recurring victimization.¹⁰⁶

The expansion and strengthening of "corporate knowledge" in the area of victim identification is crucial and fundamental to a meaningful response to victims of sexual abuse; without it, the children simply go on in their suffering. The NCECC has, as part of its mandate, the responsibility to identify victimized children. The Centre can provide a number of services to law enforcement, including expertise in victim identification techniques. This expertise must be supported and built upon.

¹⁰³ NCMEC's Child Victim Identification Program does not retain actual photos of the children. www.cybertipline.com/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=2444.

¹⁰⁴ www.ceop.gov.uk/mediacentre/statistics.asp.

¹⁰⁵ Two provinces, Ontario and Quebec, have legislative requirements mandating law enforcement agencies submit reports to the Violent Crime Linkage Analysis System (ViCLAS), an automated national database case linkage system designed to capture, collate and compare crimes of violence through the analysis of victimology, offender/suspect description, modus operandi, forensic and behavioural data. ViCLAS is operated by the RCMP and its success is dependent upon the number of officers who submit reports to it. There are over 300,000 cases on the system and over 3,000 linkages have been made, but participation is not universal.

¹⁰⁶ Ontario's Provincial Strategy to Protect Children from Sexual Exploitation and Abuse on the Internet, PowerPoint presentation, January 2008.



Responsible image management

While image databases have obviously proven useful, there is an obligation to remain conscious of the impact that the storage and sharing of these documents may have on the victims. The international organization End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes warns, “Knowledge of the existence of images in police databases may be just as harmful to the child.”¹⁰⁷ For victims, it may not matter who is looking at their photos or why they are being used. They have no control over who has access to them, if they are ever removed, etc.

The NCECC is aware of the privacy implications for victims of having their photos included in law enforcement databases and is preparing a Privacy Impact Assessment for the Federal Privacy Commissioner. The Centre will continue to dialogue with the Office of the Federal Ombudsman for Victims of Crime as policies are developed.

RECOMMENDATION 5—That the federal government, in partnership with the provinces, develop a national strategy to identify victims found in child sexual abuse images and that the strategy includes an expansion of the National Child Exploitation Coordination Centre's National Victim Identification Unit and support for the national image database.

¹⁰⁷ “Violence Against Children in Cyberspace,” ECPAT International, 2004.

6. HELPING VICTIMS HEAL

"A nine year old girl was abused by her uncle and the only reason she agreed to come to the centre was because her mom told her she would only have to tell her story once. That was one Friday afternoon. On Monday afternoon, after school, she cleaned out her piggy bank and asked her mom to take her to Toys R Us. She had enough money to buy three stuffed animals. She dropped them off at the front counter here and said, 'These are for the next three kids who come to Zebra.'"¹⁰⁸

—Barb Spencer, Executive Director, Zebra Child Protection Centre

"Not having such a centre available in other major cities defies belief; it is like the subtle difference between holding a hand and chaining a soul for the children who need this protection...."

—Mother whose son was sexually abused and who attended the Zebra Centre

Child advocacy centres: A model for success

First developed in the U.S. in the 1980s, Child Advocacy Centres (CACs) were designed to reduce the stress on child abuse victims and families created by traditional child abuse investigation and prosecution procedures and to improve the effectiveness of the response.¹⁰⁹

A victimized child and his or her family can go to more than 10 different locations and see multiple professionals before getting help.¹¹⁰

These professionals are often working in isolation and do not communicate efficiently or effectively with the child and family, or with each other. The result is a fragmented, confusing, inefficient and expensive process. CACs, on the other hand, provide an integrated approach to helping children who have been victims of abuse by bringing together key victim services, such as statement collection and counselling, in one child- and family-friendly location.

The National Network of Children's Advocacy Centers, now called the National Children's Alliance (NCA), was formed in 1988. It is a U.S. nationwide not-for-profit membership organization whose mission is to promote and support communities in providing a coordinated investigation and comprehensive response to victims of severe child abuse. There are over 900 CACs and over 600 are certified with the NCA.¹¹¹

¹⁰⁸ Jamie Hall, "Shedding light on the darkest of crime," *Edmonton Journal*, September 29, 2007.

¹⁰⁹ Theodore P. Cross et al., "Evaluating Children's Advocacy Centres' Response to Child Sexual Abuse," Office of Juvenile Justice and Delinquency Programs, August 2008. www.ncjrs.gov/pdffiles1/ojjdp/218530.pdf.

¹¹⁰ BOOST Child Abuse Prevention & Intervention.

¹¹¹ Under the U.S. federal *Victims of Child Abuse Act*, the NCA receives funds from the American Department of Justice, Office of Juvenile Justice and Delinquency Prevention, and distributes funds to local communities to support the growth, continuation and development of CAC programs nationally. Certified CACs may receive annual funding.

Although the services offered vary, there are some key elements necessary to gain accreditation from the NCA:

1. *Child-appropriate/child-friendly facility:* The CAC provides a comfortable, private, child-friendly setting that is both physically and psychologically safe for clients.
2. *Multidisciplinary team:* This multidisciplinary team for response to child abuse allegations includes representation from law enforcement, child protective services, prosecution, mental health, medicine and victim advocacy.
3. *Cultural competency and diversity:* The CAC promotes policies, practices and procedures that are culturally competent; cultural competency being defined as the capacity to function in more than one culture, requiring the ability to appreciate, understand and interact with members of diverse populations in the local community.
4. *Forensic interviews:* Forensic interviews are conducted in a neutral, fact-finding manner and are coordinated to avoid duplicative interviewing.
5. *Medical evaluation:* Specialized medical evaluation and treatment are to be made available to CAC clients as part of the team response, either at the CAC or through coordination and referral with other specialized medical providers.
6. *Therapeutic intervention:* Specialized mental health services are to be made available as part of the team response, either at the CAC or through coordination and referral with other appropriate treatment providers.
7. *Victim support/advocacy:* Victim support and advocacy are to be made available as part of the team response, either at the CAC or through coordination with other providers, throughout the investigation and subsequent legal proceedings.

8. *Case review:* Team discussion and information sharing on the investigation, case status and services needed by the child and family are to occur on a regular basis.
9. *Case tracking:* CACs must develop and implement a system for monitoring case progress and tracking case outcomes for team components.

Research suggests that these centres are having a real impact that is measurable not just in terms of its benefits to victims and their families, but in dollars.

The National Children Alliance Annual Report states that an investigation into a child abuse case in a community with a CAC is 45 percent less expensive than in a community without a CAC.¹¹²

Similarly, evaluations from the Crimes Against Children Research Center found jurisdictions with CACs allow for more coordinated investigations, higher rates of referrals for mental health services and suggest parents are more satisfied and children are less scared.¹¹³

The United Nations Resolution on Guidelines on Justice in Matters involving Child Victims and Witnesses of Crime, which Canada spearheaded, reflects many of the same principles that guide CACs. For example, the resolution recognizes that children are particularly vulnerable and “need special protection, assistance and support appropriate to their age, level of maturity and unique needs in order to prevent further hardship and trauma that may result from their participation in the criminal justice process.”¹¹⁴

¹¹² National Children Alliance Annual Report 2005. www.nca-online.org/uploads/NCA%20AR2005.pdf.

¹¹³ Crimes Against Children Research Center, “Executive Summary: Findings from the UNH Multi-Site Evaluation of Children’s Advocacy Centers.” www.unh.edu/ccrc/.

¹¹⁴ www.un.org/docs/ecosoc/documents/2005/resolutions/Resolution%202005-20.pdf.

The guidelines stress that:

- To avoid further hardship to the child, interviews, examinations and other forms of investigation should be conducted by trained professionals who proceed in a sensitive, respectful and thorough manner. Special services and protection will need to be instituted to take account of gender and the different nature of specific offences against children.
- Professionals should make every effort to coordinate support so that the child is not subjected to excessive interventions. The child should receive assistance from support persons, such as child victim/witness specialists, commencing at the initial report and continuing until such services are no longer required.

Child advocacy centres in Canada

In a report prepared for the Law Commission of Canada, researchers estimated the cost of child abuse for Canadian society in 1998—including judicial, social services, education, health, employment and personal costs—was \$15,705,910,047.¹¹⁵ They also found that in general, the major costs of child abuse are not borne by the Government, but instead are personal costs to the victims. “Our research strongly suggests that it is false economy to save dollars in the short run by ignoring abuse or by cutting programs designed to help families. There is a tremendous imbalance in what we as a society allocate to reduce the effects of abuse and the costs themselves.”¹¹⁶

“Even a relatively small increased investment in effective prevention and treatment programs could yield huge dividends for society. In fact, the earlier the intervention, the lower the overall costs and the greatest chance there is for a reduction of the multiplier effects consequent to abuse.”¹¹⁷

In Canada, only a few programs offer services similar to those of the CAC model. The Edmonton Zebra Centre (2002) is the only program currently affiliated with the NCA. Other examples of similar programs include the newly created Niagara Child Advocacy Centre (2008)—which hopes to receive accreditation from the NCA—the Regina Children’s Justice Centre (1994), the Gatehouse and the BOOST Centre in Toronto. Several other communities are exploring CACs for their jurisdictions but in some cases funding has been identified as a barrier.

The benefits of CACs in the U.S. are also being seen in Canada. The Edmonton Zebra Centre has specially trained forensic interviewers who conduct the interviews with children. Police and child welfare officers observe the interviews but do not question the child. The centre has proven that the CAC model and coordinated investigations get proven results. Specifically, it has found that the CAC model leads to a reduction in system-induced trauma for victims, an increase in charges laid, better quality of evidence, more guilty pleas and higher convictions rates with more appropriate sentences.¹¹⁸ On top of that, the Zebra Centre has also found that families are generally more willing to access services if they are on-site.

Conversely, the BOOST centre warns that, “...a lack of coordination and organization negatively affects victims who do not receive the maximum amount of benefit from services and the legal system.”¹¹⁹

¹¹⁵ Audra Bowlus, Katherine McKenna and David Wright, *The Economic Costs and Consequences of Child Abuse in Canada*, Law Commission of Canada, 2003, p. V. http://dsp-psd.pwgsc.gc.ca/collection_2007/lcc-cdc/JL2-39-2003E.pdf

¹¹⁶ *Ibid.*, p. 91.

¹¹⁷ *Ibid.*, p. 92.

¹¹⁸ ZEBRA Child Protection Centre, *Victims of Crime Fund Grants Program Evaluation Report*, March 1, 2007, p. 9.

¹¹⁹ BOOST Child Abuse Prevention & Intervention, “Responding to Child & Youth Victims of Sexual Exploitation on the Internet: Best Practice Guidelines.” www.boostforkids.org, p. 15.

How child advocacy centres can help victims of Internet-facilitated child sexual abuse

Given the unique dynamics surrounding child sexual abuse images and the benefits of a coordinated approach, CAC models could be particularly relevant in investigations involving child sexual abuse images. They could help to obtain more information from children (i.e. existence of photos), recognize the signs of when a child may not be disclosing, and provide guidance on how to handle a situation where images have been found but the child is not disclosing or not aware, and more.

According to BOOST, interviewing victims of child sexual abuse imagery crimes may require a different strategy, compared to conventional sexual abuse:

“Due to the fact that abuse imagery on the Internet is a permanent record of maltreatment, children in these situations often do not disclose full details of the abuse until they have recovered from the initial trauma of realizing that others will see the pictures in the future. In addition, child abuse imagery is physical evidence of a crime scene, and thus, investigators aim to acquire knowledge about the offender(s) and not the crime itself. Consequently, when investigators (and treatment providers) speak with children, interviews should span over a period of weeks to months. Questions should be general in nature, focus on the offender(s)’ identity, and the possibility of other children currently being victimized; they should not discuss details of the abuse; and, they should not focus on the nature of the abuse, as those working with the children will already know what has happened, and discussing the abuse will be psychologically harmful for the child.”¹²⁰

Some of this work is already underway. The Northern Alberta Integrated Child Exploitation (ICE) Team actively works with the Zebra Centre to help victims of child sexual abuse.



¹²⁰ Ibid.

It is clear from the evidence that CACs are a proven, results-oriented and victim-friendly way to ensure better victim care, higher conviction rates and lower systemic costs.

For that reason, the Federal Ombudsman for Victims of Crime wrote to the Minister of Finance in advance of Budget 2009 to request that \$5 million be allocated toward the support of these centres across the country. While the recommendation was not included in the January budget, there is still an opportunity for the federal government to take action.

RECOMMENDATION 6—That the federal government, in conjunction with provincial and municipal governments, develop a national strategy to expand the network of Child Advocacy Centre models in communities across the country.¹²¹

7. LEARNING TO BETTER HELP VICTIMS

"Long term effects of being photographed were more debilitating...exacerbated by the knowledge that others may see or distribute the films...knowledge that photos may be used to exploit other children."¹²²

"Little is known about the full and long term impact of being used in pornography upon children and their families, their coping strategies and the support they do or do not receive."¹²³

Therapists, law enforcement and victim services have years of experience dealing with child sexual abuse victims, but there is growing recognition that the making of child sexual abuse images and their distribution complicate the aftermath of the sexual abuse. This has an impact on the recovery of victims and the delivery of services to those victims.

"Due to its relatively new nature, the Internet adds novel and specific elements of victimization that have never been present in the past. Of particular concern is the fact that the Internet provides a permanent, uncontrollable record of abuse; if child sexual abuse images or videos of victimization exist on the Internet, they will never disappear. This aspect of victimization has devastating effects on victims including: victim silencing; self-blame for the abuse; increased levels of trauma; shame and embarrassment knowing that others have/will see the abuse on the Internet; decreased amounts of disclosure; and, victims taking a longer amount of time to recover from the abuse in comparison to exploitation without recording."¹²⁴

Given these complications, it is necessary that the professionals who are helping victims and their families learn more about dealing with this particular type of abuse, methods for coping and signs of further distress.

¹²¹ It is important to emphasize the importance of community involvement in developing a CAC and that no one model will work for every community.

¹²² M.H. Silbert, *Effects on Juveniles of Being Used for Pornography and Prostitution*, in D. Zilman and J. Bryant (eds.), *Pornography: Research Advances and Policy Considerations*, Lawrence Erlbaum Associates, 1989.

¹²³ Susan J. Creighton, "Child pornography: images of the abuse of children," November 2003. www.nspcc.org.uk.

¹²⁴ BOOST Child Abuse Prevention & Intervention, "Responding to Child & Youth Victims of Sexual Exploitation on the Internet: Best Practice Guidelines." www.boostforkids.org, p. 1.

Dr. Sharon Cooper recommends that those who work with child sexual abuse victims,

“...have to learn how to ask the right questions about the possibility that a child’s victimization may have entailed production, dissemination, possession or extortion through the use of child sexual abuse images...” because “...children not only typically do not tell of their abuse, but will in fact deny the presence of images.... This background of having pictures and videos taken of one’s sexual abuse is a significant risk factor for substance abuse, mental health problems and run away behaviours.”¹²⁵

Recently, the Supreme Court of Canada recognized the additional suffering that the distribution of child sexual abuse can cause when it reinstated a more severe sentence for a father who was convicted of sexually assaulting his 4-year-old daughter and of making, distributing and possessing child pornography. At the time of his arrest, his computer contained approximately 5,300 pornographic photographs and 540 pornographic videos involving children, many of which included his daughter. The trial judge imposed the maximum sentence of 10 years for sexual assault and another 5 years for the other offences but the Court of Appeal reduced the sentence from 15 to 9 years. Supreme Court Justice LeBel said, “I note that L.M. disseminated his pornography around the world over the Internet. The use of this medium can have serious consequences for a victim. Once a photograph

has been posted on the Web, it can be accessed indefinitely, from anywhere in the world. R.M. will never know whether a pornographic photograph or video in which she appears might not resurface someday.”¹²⁶

At the victims’ level, a psychological assessment and treatment model is being developed for children and their families as part of the Ontario Provincial Strategy to Protect Children from Sexual Abuse and Exploitation on the Internet.¹²⁷ Additionally, the Ontario Victim Services Secretariat at the Ministry of the Attorney General offers a program to pay for counselling for young victims of sexual exploitation on the Internet who were under the age of 18 when the crime took place. The program also helps their family members. Over 385 victims have been assisted in Ontario and over 90 people have accessed the special compensation fund to assist victims and their families to access counselling.¹²⁸

Answering tough questions

The problem is that there has been little research into these issues. According to BOOST, “Among many regions, there is a lack of understanding about the experience of victims who have been sexually exploited on the Internet... compared to other forms of child maltreatment, there is a relatively small amount of research and literature about Internet child exploitation.”¹²⁹

¹²⁵ Dr. Sharon Cooper, Oral Testimony for the United States Senate Committee on Commerce, Science and Transportation, September 19, 2006.

¹²⁶ *R. v. L.M.*, 2008 SCC 31, para. 28. This case resulted from an investigation by Switzerland police into groups distributing child sexual abuse images on the Internet. Switzerland police alerted Quebec authorities about the two Quebecers who had been identified in Internet user groups. Had this investigation into the distribution of child sexual abuse images not taken place, a father would still be abusing his daughter today.

¹²⁷ Dr. Jennifer Coolbear and Tanya Smith, Toronto Hospital for Sick Kids, BOOST—Responding to Child and Youth Victims of Sexual Exploitation on the Internet Conference, Collingwood, Ontario, September 2007. Part of the strategy includes coordinating the identification of victims and providing support services, and Ontario has developed a special compensation program for victims and has provided compensation to over 300 victims.

¹²⁸ Direct victims may receive up to \$1,500 for counselling and family members may receive up to \$800.

¹²⁹ BOOST Child Abuse Prevention & Intervention, “Responding to Child & Youth Victims of Sexual Exploitation on the Internet: Best Practice Guidelines.” www.boostforkids.org, p. 11.

Despite the successes, the relatively small number of victims who have been identified and their young age, combined with the lack of experience with the long-term impacts that these images may present, means there are many questions but few satisfactory answers at this time. So far, much of the work victim services have done is with adolescent females who have been targeted by adult men online, and these cases may present entirely different dynamics than cases involving images and abuse.¹³⁰

More work needs to be done to answer some important questions. What should be done when victims have grown up but are unaware that images were made? What should happen when law enforcement discovers old images? Should those victims be notified (if they are identified)? If so, how? At what age? What if a child does not disclose that images were made? If a child denies the images or videos, should the child be challenged?

As Jonah Rimer stated, “Very little is known about the psychological effects on adults who are told that there are child abuse images of them on the internet and careful thought must go into the time and way in which such a revelation should take place.”¹³¹

There are also the questions that surround victims who know already that these images exist. Victims may be concerned about how those viewing the images (i.e. police officers) may perceive them. Many abusers force victims to appear as if they are enjoying what is happening, and therefore a victim may be concerned that police will think they really enjoyed it. Child sexual abuse images and videos may, in some cases, challenge the perceptions and beliefs that authorities have of child sexual abuse

victims (i.e. that they are always non-compliant victims forced to perform).

Retired FBI Agent Kenneth Lanning said, “Society has a problem dealing with any sexual-victimization case in which...the child victim is not completely good. The idea that child victims could simply behave like human beings and respond to the attention and affection of offenders by voluntarily and repeatedly returning to an offender’s home is a troubling one. It confuses us to see the victims in child pornography cases giggling or laughing.”¹³²

The international organization End Child Prostitution, Child Pornography and Trafficking of Children for Sexual Purposes also makes the point that “Practitioners report that a child in this situation may feel that the existence of imagery of their humiliation masks the violence they have experienced and makes them appear complicit. This dilemma adds an extra traumatic burden.”¹³³

Sexual abuse is never the child’s fault as they are legally incapable of consent. But for some victims, the abuse has become so normalized that they have adopted coping methods that may shock us. One investigator described one case where he saw the grooming of a victim, which started with taking normal photos, then led to harmless play, culminating in sexual abuse. At the “end” of the process, the victim was directing some of the abuse, negotiating for presents or money to participate and perform certain acts.

For these reasons and more, victims often do not disclose that photos were taken or videos were made. Even when confronted with such discoveries, some victims will

¹³⁰ For example, some of these teens may not identify themselves as victims. In a high-profile case involving a Kingston man who manipulated hundreds of girls worldwide into performing sexual acts in front of a webcam and threatened them with exposure of the images, law enforcement reports that some of the girls did not think it was that serious. It remains to be seen what the long-term impacts of such victimization may be.

¹³¹ Jonah Rimer, *Literature Review—Responding to Child & Youth Victims of Sexual Exploitation on the Internet*, 2007, p. 52.

¹³² Kenneth V. Lanning, “Overview of Sexual Victimization of Children,” adapted from the National Center for Missing and Exploited Children, *Child Molesters: A Behavioural Analysis* (4th ed.), 2001.

¹³³ ECPAT International, “Violence Against Children in Cyberspace,” 2005. p. 41.

refuse to acknowledge their existence. Children “can easily suffer further harm if they are pressured to verify the authenticity of an abuse image.”¹³⁴

This must be taken into consideration when law enforcement makes a decision on how to approach child victims to learn more information about the offender or the crime.

Law enforcement techniques that may be helpful in traditional child sexual abuse cases need to be re-examined in cases involving child sexual abuse images. For example, police often videotape children giving statements in cases of child sexual abuse. In Canada, these videos may be used in court and can be beneficial to the prosecution of child sexual abuse cases. But concerns have been raised that “...taking video evidence from a child already forced to make abuse images could further the harm done to the child.”¹³⁵ For children who have been the subject of abusive images, the use of a televised link may trigger memories or flashbacks to their abusive experiences.

All in all, it is clear that a lot of work needs to be done to help law enforcement, psychologists, counsellors and other key professionals understand how best to help victims of Internet-facilitated child sexual abuse.

RECOMMENDATION 7—That the Department of Justice's Policy Centre for Victim Issues fund research into the needs of victims of Internet-facilitated child sexual abuse.

8. ENDING ONGOING VICTIMIZATION

“This is how I see it. When I capture their image—I capture a piece of time that not even there own mommy's will have. They stay young forever, just for us pedos.... The vid cam makes them our eternal slaves. They becum our property to do whatever we want too.”

—Written in a chat message by Darren Philpott/canuckboylover¹³⁶

“Usually, when a kid is hurt and the abuser goes to prison, the abuse is over. But because XXX put my pictures on the Internet, the abuse is still going on.... I am more upset about the pictures on the Internet than I am about what XXX did to me physically.”

—13-year-old sexual abuse victim whose images were put on the Internet

As determined, the ongoing circulation of child sexual abuse images makes it exponentially more difficult for victims to move on and heal.

While the abuse itself may have taken place in the past, victims are continually traumatized by the fact that those images continue to circulate and be used for gratification purposes. This is compounded by the fear that such personal markers of their own private past could pop up anywhere, for anyone to see at any given time.

¹³⁴ Ibid., p. 42.

¹³⁵ Ibid., p. 42.

¹³⁶ Jana G. Pruden, “He’s dead, but the abuse lives on...,” *Leader-Post*, November 22, 2008. Philpott was awaiting trial on child pornography and child sexual abuse when he committed suicide.



Such ongoing levels of anxiety would be difficult for anyone to bear. For a victim who not only feels the embarrassment and shame of the image itself, but is forced to relive the crime each time the image is viewed, it is excruciating.

Consequently, it is imperative that any consideration of this issue include a discussion and recommendation on the handling of child sexual abuse images once they have been identified.

The handling of images falls into two main spheres—the lawyers and law enforcement specialists who handle and store the images as evidence and the Internet itself where the images are circulating.

Handling of child sexual abuse images in the Canadian justice system

In Canada, Crown attorneys are obligated to disclose copies of all evidence to the defence, including child

sexual abuse images. These images are, however, unique and, given the serious privacy implications that exist for such victims, special care must be taken with respect to their disclosure.

This has already been recognized in the U.S. where legislation provides that in child pornography prosecutions, any property or material that constitutes child pornography shall remain in the care, custody and control of either the Government or the Court and that courts shall deny any request by the defendant to copy, photograph, duplicate or otherwise reproduce any property or material that constitutes child pornography so long as the Government makes the property or material reasonably available to the defendant.¹³⁷

In 1993, the Ontario Attorney General's Advisory Committee on Charge Screening, Disclosure and Resolution Discussions ("the Martin Committee") recognized that while the "normal method" of disclosure was by copy, other interests, including

¹³⁷ Title 18, section 3509 of the U.S. Code.

a reasonable privacy or security interest of a victim or witness, may require and allow for an alternative form of disclosure, such as private viewing.¹³⁸

In *R. v. Blencowe*, which involved the disclosure of 35 videotapes alleged to contain child pornography, Mr. Justice Watt found that while disclosure to defence counsel was mandatory, it was also necessary to consider the privacy interests of the victims and that they not be further compromised by copying, viewing, circulation or distribution of the tapes beyond what was required. Justice Watt required defence counsel to sign an undertaking with certain conditions prior to receiving disclosure. He proposed several conditions, including that counsel retain possession and control of the copies and not release them to anyone other than an expert; that the defendant not have possession or control of the tape (or images); that no one be permitted to view the tapes (or images) except the applicant, his counsel and any expert; that no copies be made and that the tape (or images) be returned to the investigating officer.¹³⁹

More recently, in October 2008, an Alberta Provincial Court judge imposed strict conditions for the defence lawyer to abide by upon receipt of the DVD from the Crown: A lengthy password, which could not be written down, was given to him so he could access the evidence on the encrypted DVD; he could not allow anyone else to view the evidence; the DVD had to be returned to the Crown for destruction; and finally, he had to turn over the computer used for viewing the evidence to have an expert delete everything.¹⁴⁰

In Canada, defence attorneys may be required to enter into an undertaking or to apply for a court order under subsection 490(15) of the *Criminal Code* to obtain access to the seized images, pursuant to conditions similar to those set out above (although more stringent).¹⁴¹ Unfortunately, an undertaking is no guarantee that a child's privacy will not be compromised. On at least two occasions, defence counsel in Ontario have lost or misplaced material and were not able to return it to the police.

Finally, once the evidence has been viewed and removed it should be deleted from the original computer system in accordance with the *Criminal Code*. Subsection 164.1(5) of the *Criminal Code* allows the Court to make an order to the "custodian of the computer system" to delete material that the Court is satisfied, on a balance of probabilities, is child pornography.¹⁴² There is little evidence, however, to show that courts are making these orders. We therefore urge the Department of Justice to consult with its provincial and territorial counterparts to determine if these provisions are being used as Parliament intended and if they need to be amended to provide more clarification for the Court.

RECOMMENDATION 8—That the federal government introduce legislation to amend the *Criminal Code* to ensure that child sexual abuse images, video or audio recordings are not disclosed to defence counsel but that opportunities are made available for proper review of the evidence.

¹³⁸ *Report of the Attorney General's Advisory Committee on Charge Screening, Disclosure and Resolution Discussions*, 1993, pp. 235–236.

¹³⁹ *R. v. Blencowe* (1997) O.J. No. 3619.

¹⁴⁰ "Lawyer can view alleged child porn," *Calgary Herald*, October 24, 2008.

¹⁴¹ Subsection 490(15) of the *Criminal Code* provides for a court to make an order allowing a person who has an interest in items seized by the police to examine anything so detained. Subsection 490(16) provides for the court to place conditions on the order allowing access in order to safeguard and preserve the items in question. Section 605 provides a mechanism for the courts to balance competing interests and impose conditions when contraband is released to defence counsel (i.e. guns or drugs released for scientific testing) pursuant to section 605 of the *Criminal Code*.

¹⁴² According to a 2001 Department of Justice background, Bill C-2 suggests "custodian of a computer system" includes ISPs.

9. STEMMING THE FLOW OF CHILD SEXUAL ABUSE IMAGES OVER THE INTERNET

"The simplicity of getting material...it's close to mind-boggling. I have never understood how come the whole thing wasn't shut down. You search for the word 'baby' and it will find stuff there...it's easy...."

—Michael Briere, murderer of Holly Jones¹⁴³

"I never escape the fact that pictures of my abuse are out there forever. Everything possible should be done to stop people looking at pictures of child abuse. Each time someone looks at pictures of me, it's like abusing me again.¹⁴⁴"

—16-year-old girl named Sandra

"Growing up and trying to fit into a normal life after so much abuse is hard. I have nightmares, flashbacks and struggle with everyday tasks that most people take for granted.... There is a haunting that surrounds me constantly, reminding me that I don't have control over keeping my past a secret. The pictures that were taken when I was so young are still out there. Who knows where they are and how many people have seen them. I wonder if they will show up when I least expect it. I am away from abuse now, but know that someone could be pleasuring himself while looking at my pictures or showing them to kids."

—A victim¹⁴⁵

There is unfortunately no magic button or software that can locate and destroy all child sexual abuse images on the Internet. Once an image is released, it is impossible to get back. The image becomes part of an endless cycle of abuse as it is shared by countless predators and may be used to groom other victims.

That being said, there are measures that can be taken by both government and the private sector to help curb the spread of the material and deter abusers from accessing it.

At the 2007 G8 Justice and Home Affairs Ministers meeting, all Ministers recognized that the war against Internet predators could not be won by law enforcement alone.¹⁴⁶ They acknowledged that the private sector has an important role in protecting the world's children.

Working with the private sector

There are some positive examples of industry leaders accepting responsibility for their role in preventing the spread of child sexual abuse images. For example, AOL—an online service provider—developed the Image Database and Filtering Process, which allows AOL to proactively and automatically locate known child sexual abuse images moving through its system, delete them and route a report to law enforcement.¹⁴⁷ In one of its first cases, AOL notified the NCMEC that an AOL user had tried to upload a single image to his email account. Within a week, the local police had a search warrant and arrested a California man. His arrest led to the identification of 35 other people involved in trading images. On top of it, the California man, who was a youth baseball coach, admitted he had abused a child.

MSN uses a filtering tool to review images uploaded to MSN Spaces and MSN Groups. Images that are flagged as potential child sexual abuse images are reviewed and,

¹⁴³ Canadian Press, "Michael Briere says he was spurred by kiddie porn in sex slaying of Holly Jones," *Peterborough Examiner*, June 18, 2004.

¹⁴⁴ Internet Watch Foundation.

¹⁴⁵ Monique Mattei Ferraro and Eoghan Casey, "Investigating Child Exploitation and Pornography," Elsevier Academic Press, 2005, p. 3.

¹⁴⁶ G8 Justice and Home Affairs Ministers, May 24, 2007. www.g8.gc.ca/childpornography-en.asp.

¹⁴⁷ Julian Sher, *Caught in the Web*, Perseus Publishing, 2007, p. 232.

if deemed appropriate, a report is sent to the NCMEC.¹⁴⁸ MSN closes the site and preserves the entire site, account information and associated files.

This software used by MSN and AOL focuses on images that are a part of the NCMEC database. The technology is not a cure-all as it does not apply to new images, but it is an important first step. If all ISPs participated, it could have an impact on the child sexual abuse image industry as a whole by helping to prevent the dissemination of child sexual abuse images, thereby preventing further exploitation of some victims.

The same type of technology could be developed in Canada to identify and remove images that are found within the Canadian NCECC child sexual abuse imagery database. By blocking the dissemination of these photos, Canada could have a real impact on stemming the flow of these abusive images.

Project Cleanfeed is another example of a successful private initiative. The U.K.-based filter helps participants, such as British Telecom, to block approximately 35,000 attempts to visit illegal child abuse sites every day.¹⁴⁹

Cybertip.ca, run by the Canadian Centre for Child Protection,¹⁵⁰ operates a Canadian Cleanfeed project and provides a list of specific foreign-hosted Internet addresses associated with images of child sexual abuse to participating ISPs.¹⁵¹ These ISPs then use the technology to filter or prevent access to those sites. On average, Cybertip.ca receives over 700 reports and 800,000 hits to its website per month. The reports have resulted in dozens of arrests, the eliminations of thousands of websites and the rescue of numerous children.

In Canada, some companies voluntarily participate in Project Cleanfeed to block foreign websites hosting prepubescent images.¹⁵² Unlike the U.K., Canada's Cleanfeed targets

¹⁴⁸ Philip K. Reiting, *Written Congressional Testimony—Making the Internet Safe for Kids: The Role of ISPs and Social Networking Sites*, June 27, 2006.

¹⁴⁹ BBC News, February 7, 2006.

¹⁵⁰ Canadian Centre for Child Protection, a charitable organization dedicated to the personal safety of all children.

¹⁵¹ In the U.K., the Internet Watch Foundation provides the list.

¹⁵² Cybertip reports domestic sites to Canadian law enforcement agencies.

only “prepubescent” material so that participating ISPs do not unintentionally block legal sites that include females over the age of 18 (many of whom are advertised as looking younger).¹⁵³

As of February 2009, only eight of the more than 400 ISPs in Canada participated in Cleanfeed Canada.¹⁵⁴ Fortunately, most of the largest ISPs, such as Telus and Bell, do participate, which means that almost 90 percent of all Canadian Internet subscribers are covered by the Cleanfeed program. While those ISPs that are voluntarily participating should be congratulated, **every** ISP in Canada should be obligated to participate in this initiative.

Since 2006, there have been 13,000 URLs¹⁵⁵ added to Cybertip.ca’s list. Almost half of these sites involve sexual acts with children and almost 90 percent involve children under 8.¹⁵⁶ One ISP identified 2,900 attempts in a 24-hour period to access a blocked website.¹⁵⁷ Despite these statistics, it is important to keep in mind that 80 percent of millions of sites still leaves hundreds of thousands accessible.

There are those who will argue that stricter laws or filters interfere with regular, legitimate sites. Cybertip.ca has addressed this by putting in place a thorough appeal process for someone who feels legal material has been blocked.

Furthermore, the potential negatives of having stronger filters or a more restrictive approach are generally limited to prohibiting access to a site that advertises adult females who look like they might be 12. Given the extensive appeal process, we do not believe this current limitation is justifiable.

RECOMMENDATION 9—That the federal government introduce legislation to require all ISPs to block access to sites containing images of children who are or are depicted as being under the age of 18 years, and block the distribution of known child sexual abuse images based on images collected by the National Child Exploitation Coordination Centre.

¹⁵³ The U.K. list includes any site that contains potentially illegal child sexual abuse content that would be an offence to download (make).

¹⁵⁴ www.cybertip.ca/app/en/cleanfeed_p2#anchor_menu.

¹⁵⁵ A URL (Uniform Resource Locator) is the unique address for a file that is accessible on the Internet. For example, to get to a website, you can enter the URL of the home page in your Web browser’s address line.

¹⁵⁶ Signy Arnason, Cybertip.ca, Ontario Provincial Strategy to Protect Children from Sexual Abuse and Exploitation on the Internet Multi-disciplinary Conference, November 18, 2008, London, Ontario.

¹⁵⁷ Noni Classen, Canada Centre for Child Protection, BOOST—Responding to Child & Youth Victims of Sexual Exploitation on the Internet Conference, Collingwood, Ontario, September 2007.



"We have an opportunity to stop the continual trauma experienced by victims of Internet-facilitated sexual abuse by treating these images as what they are—ongoing abuse."

Conclusion

THIS REPORT HAS IDENTIFIED A NUMBER OF SIZABLE GAPS where children are falling through the cracks and offenders are gaining momentum. *Each of these gaps represents an opportunity to act; to make positive change and to protect vulnerable children.*

There is an opportunity to better communicate the horror of the problem by moving away from the term "child pornography" to more accurate terms such as "child sexual abuse images" or "child sexual abuse videos."

We have an opportunity to help dedicated law enforcement professionals more effectively find the offenders *and* victims of these abuses by giving them the tools they need to pursue investigations—including the ability to obtain simple customer name and address information, to access computers that have been seized regardless of password protections or encryptions, and to provide support and resources to finding better and more efficient ways to analyze images.

In cases where law enforcement is able to identify and rescue victims, there is an opportunity to make a difference in victims' lives by fostering a stronger understanding of their needs and responding with effective, victim-friendly services.

Finally, we have an opportunity to stop the continual trauma experienced by victims of Internet-facilitated sexual abuse by treating these images as what they are—ongoing abuse. By ceasing the disclosure of images and by making private sector ISPs more accountable, there is an opportunity to spare a child one more humiliation.

We request the Ministers of Justice, Public Safety and Industry and affected agencies to consider these opportunities and recommendations and to report back to the Office of the Federal Ombudsman for Victims of Crime. We look forward to the Government's action plan, detailing how it will move forward to enhance the protection of children.



Appendix 1

List of recommendations

Recommendation 1

That the federal government introduce legislation to amend the child pornography provisions in the *Criminal Code* to provide a more accurate description of the crime (i.e. such as child sexual abuse images, child sexual abuse videos, child sexual abuse writings) to ensure a more accurate reflection of the harm that is done to victims.

Recommendation 2

That the federal government expedite legislation to require ISPs to provide customer name and address information to law enforcement.

Recommendation 3

That the federal government introduce legislation to require ISPs to retain customer name and address data, traffic data and content data for two to five years.



Recommendation 4

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.

Recommendation 5

That the federal government, in partnership with the provinces, develop a national strategy to identify victims found in child sexual abuse images and that the strategy includes an expansion of the National Child Exploitation Coordination Centre's National Victim Identification Unit and support for the national image database.

Recommendation 6

That the federal government, in conjunction with provincial and municipal governments, develop a national strategy to expand the network of Child Advocacy Centre models in communities across the country.

Recommendation 7

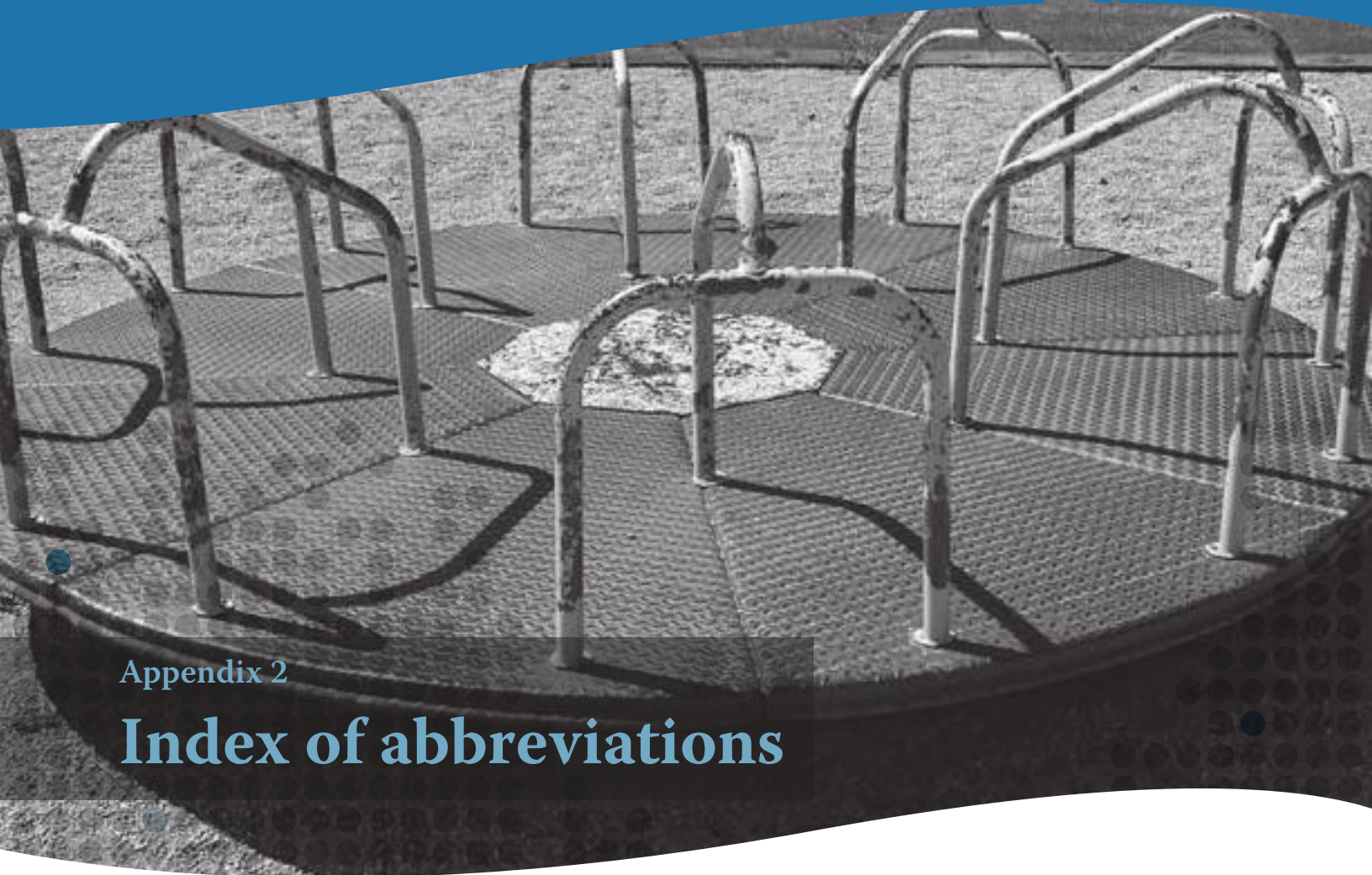
That the Department of Justice's Policy Centre for Victim Issues fund research into the needs of victims of Internet-facilitated child sexual abuse.

Recommendation 8

That the federal government introduce legislation to amend the *Criminal Code* to ensure that child sexual abuse images, video or audio recordings are not disclosed to defence counsel but that opportunities are made available for proper review of the evidence.

Recommendation 9

That the federal government introduce legislation to require all ISPs to block access to sites containing images of children who are or are depicted as being under the age of 18 years, and block the distribution of known child sexual abuse images based on images collected by the National Child Exploitation Coordination Centre.



Appendix 2

Index of abbreviations

CAC –	Child Advocacy Centre	ISP –	Internet Service Provider
CCAICE –	Canadian Coalition Against Child Exploitation	KINSA –	Kids Internet Safety Alliance
CEOP –	Child Exploitation and Online Protection Centre	NCA –	National Children's Alliance
CNA –	Customer Name and Address Information	NCECC –	National Child Exploitation Coordination Centre
FINTRAC –	Financial Transactions and Reports Analysis Centre of Canada	NCMEC –	National Center for Missing and Exploited Children
ICAID –	INTERPOL Child Abuse Image Database	OPP –	Ontario Provincial Police
ICE –	Integrated Child Exploitation Team	PIPEDA –	<i>Personal Information Protection and Electronic Documents Act</i>
IP –	Internet Protocol	RCMP –	Royal Canadian Mounted Police