THE CENTRE FOR INNOVATION LAW AND POLICY
WHITE PAPER

Safely Connected: Strategies for Protecting Children and Youth from Sexual Exploitation Online

A project of the Microsoft Safe Computing Program

October 2005

CENTRE FOR
INNOVATION LAW
AND POLICY

TABLE OF CONTENTS

PREAMBLE

The Centre for Innovation Law and Policy offers this white paper on strategies to reduce the incidence of online child exploitation, based upon the papers presented at the International Symposium on Online Child Exploitation (ISOCE) held on May 2nd, 2005 at the University of Toronto, and a roundtable discussion held on May 3rd, 2005. We are grateful to the experts who participated in these events, each of whom is listed in Appendices A and B to this report.[1] *In particular, we would like to thank David Butt for his extraordinary commitment to this project.*

The ISOCE brought together experts from diverse disciplines and fields in order to come to a better understanding of the issues associated with two problems: a) the online trade in child pornography images, and b) adults meeting young people online for sexual purposes. The Centre brings extensive experience, knowledge and expertise in technology-related policy to these problems, and organized the ISOCE as part of the Microsoft Safe Computing Program, a long term project of the Centre.

The mission of the Centre is to help foster a legal and policy environment in Canada and internationally that promotes ethical and socially beneficial innovation and technological progress. As part of this year's focus on online child exploitation, the Centre provided research support to the Ontario Attorney General's Working Group on Internet Crimes Against Kids, facilitated discussions between the Working Group, police services, and members of the Internet Service Provider (ISP) industry, designed a survey of ISPs voluntary efforts to combat online child exploitation, and held the above ISOCE. This white paper is the outcome of these year long efforts.

As the organizer of these events, the Centre has prepared this summary report of the major concerns raised by participants, along with the ideas expressed for addressing them. Participants in the ISOCE did not uniformly agree on the topics included herein. In no case should any particular participant be assumed to have concurred in any specific proposed solution.

Participants in the ISOCE and roundtable discussion appreciate the difficulty in effectively addressing these and other Internet related crimes. We encourage those in a position to implement these recommendations to see them as a means to strengthen existing efforts. We welcome this opportunity to lend our collective expertise to the project of ensuring that children and young people are kept safe from exploitation both online and offline, so that they may truly garner the many benefits that the Internet has to offer.

The Centre is grateful to Andrea Slane for her great efforts supporting the program and, in particular, as principle author of this report.

The Centre for Innovation Law and Policy

Richard Owens, *Director*

Andrea Slane

[1] The appendices to this report are available online at http://www.innovationlaw.org/English/Child-Exploitation-Appendices.html.

COMBATTING ONLINE CHILD EXPLOITATION:
RECOMMENDATIONS FOR POLICY AND LEGISLATIVE REFORM

The use of the Internet to perpetrate the sexual exploitation of children and young people is a growing problem. These recommendations, if implemented, would provide effective responses to the problem. The report presents four approaches: international co-operation in investigations, advanced training for police forces and prosecutors, corporate citizenship of Internet Service Providers, and educational programs for young Internet users.

1. International Harmonization

Canadians have been actively involved in combating online child exploitation at the international, national, provincial and local levels. However, the following areas need immediate attention:

(a) Consolidation of databases:

Databases containing the unique digital hash values[2] of known child exploitation images are a valuable resource and investigative tool for law enforcement which they can use, provided they are equipped with the appropriate software tools, to quickly analyze the contents of a suspect's computer hard drive or to sift through images in shared file sharing directories for known child pornography images. Such databases would also be useful in distinguishing images of children who have been identified from those that have not been identified. Therefore:

(i) Canada should establish a national hash value library and known image database.

(ii) The database should be linked to international efforts to coordinate national databases.

(b) Mutual Legal Assistance Treaties (MLATs):

MLATs facilitate the use of evidence gathered by foreign law enforcement services in Canadian courts. MLATs currently in force are outdated, and so not able to deal with electronic data evidence necessary for the prosecution of online crimes. Therefore:

(i) Canada should take a leading role in the process of updating these treaties, so that traffic data, IP address use logs, chat logs, and so forth collected by foreign agencies are usable in Canadian courts.

(c) Investigative information sharing:

International information sharing at the investigative stage, for example through the Child Exploitation Tracking System (CETS), likewise needs proactive attention by Canada and

[2] Hash values are unique identifying strings of characters, which measure the size and structure of a disk, a file, or a folder. They are commonly referred to as "digital fingerprints" or "digital DNA".

other national governments. As the first national host of CETS, a data sharing tool developed jointly by Microsoft Canada Co., the Royal Canadian Mounted Police and Toronto Police Services, Canada is well placed to show leadership by forging the legal instruments necessary to allow functional investigative information sharing internationally, which could then serve as a model for other nations.

(d) Sentencing:

Canada's record on sentencing offenders convicted of online child exploitation crimes shows that Canada is among the more lenient countries. Too-lenient sentencing leads to the public perception that child pornography possession, for instance, is not a serious crime. Too-lenient sentences for online child exploitation consequently do not serve to deter those people who might not commit these crimes if they feared the consequences. Therefore:

(i) Sentencing guidelines should be established to guide the judiciary in dealing with the seriousness of these crimes.

(ii) These sentencing guidelines should stress that the mandatory minimum sentences recently set for select child exploitation crimes in Bill C-2, which received Royal Assent on July 20, 2005, are the low end of the sentencing scale for child pornography crimes. The judiciary should be encouraged to send the message that all child pornography offences are serious offences that cause the abuse of children.

(e) Statutory Sexual Offences:

Canada's age of consent is currently 14, younger than the international norm. Recent efforts to enhance protection of young people between the ages of 14 and 17 include the addition of "exploitative" relationships to prohibited sexual relationships involving young people over 14, as undertaken in the amendments to the Criminal Code ushered in by Bill C-2. We recommend:

(i) The definition of "exploitative" relationships must be clarified in the amendments to the Criminal Code via official commentary, so as to capture manipulation of the affections of young people for sexual purposes.

(ii) The introduction of an online grooming offence should be studied, where knowingly sending pornographic materials, especially child pornography, to a person under 14 would be an offence.

2. Resources and Training for Police and Prosecutorial Services

Canada has several specialized units dealing with Internet crimes (or more specifically online child exploitation) that have been successful at improving efforts to combat these crimes. Further efforts are needed in the following areas:

(a) <u>Police training regarding online meeting crimes:</u>

Many online meeting crimes where young people meet adults for sexual purposes occur with the complicity of the young person. Therefore:

(i) Police need to be educated about techniques for dealing with young victims who do not feel victimized.

(ii) Youth advocates and peer support programs should be established to deal with the complex emotional issues these victims tend to encounter.

(b) <u>Police training regarding child pornography</u>

Most child pornography, especially that involving pre-adolescent children, is produced in the context of traditional child abuse situations, involving family members or close acquaintances. Therefore:

(i) Police units involved in policing online child exploitation should be connected to offline child abuse prosecution efforts.

(ii) Officers working on child abuse cases not involving the Internet should be on the lookout for child pornography that may have been produced.

(iii) Young offenders involved in trading or collection of child pornography should be treated as requiring counselling, and the possibility of the youth having been abused him- or herself should be investigated.

(c) <u>Special prosecutors:</u>

Evidence in online child exploitation crimes is often of a technical nature. Therefore:

(i) Special prosecutors with experience in prosecuting these crimes should be handling these cases, in order to best make the evidence clear to the judiciary.

(d) <u>Collaboration with industry:</u>

Collaborative efforts between Internet Service Providers (ISPs), law enforcement and government have been successful in finding some solutions to pressing issues, such as how to get subscriber information more expeditiously into the hands of law enforcement officers investigating online child exploitation crimes. Therefore:

(i) These collaborative approaches should continue to address issues as they arise.

(ii) Further collaborations should be initiated with hardware and software developers.

The Role of Internet Service Providers and Related Industries

Most Internet related businesses have been receptive to finding ways to help law enforcement pursue perpetrators of online child exploitation crimes. In order to encourage all members of the industry to follow this lead, we recommend the following:

(a) Encouraging effective self-regulation:

ISP industry associations (ISPAs) are effective means of communicating with a large number of ISPs, and for working toward common business practices. However, not all ISPs are members of such organizations. Therefore:

(i) Means of communicating with ISPs that are not members of industry associations should be found. These means should include mailings to non-members based on lists compiled from Internet resources by a government funded researcher, lists compiled by ISPAs, and/or based on business name registrations.

(ii) ISPAs should be encouraged to initiate a trust certificate program, where members would receive a seal of approval if their services include certain child protection features.

(b) Raising awareness of measures ISPs can take to help reduce these crimes:

ISPs are, by virtue of Internet technology, in the position of intermediary between law enforcement and subscribers. Therefore ISPs are in a unique position regarding the following:

(i) *Educating subscribers:* ISPs are in a unique position to educate subscribers regarding online child exploitation. Therefore:

(A) Information for children, young people, and parents should be disseminated to ISPs, who could in turn make this information available to subscribers.

(B) ISPs should help in publicizing the national tipline, cybertip.ca, to subscribers.

(C) ISPs can help disseminate information to their subscribers regarding the legal parameters of online child exploitation crimes. However, these businesses cannot be expected to be the experts on criminal law. Therefore:

(1) A government sponsored online resource should be established to provide information about what child pornography is, what activities are illegal (including accessing, downloading, sharing, emailing), and what to do if you happen upon child pornography images.

(2) This resource could also provide information on statutory sexual offences, in order to clarify for the public what is illegal about meeting a young person online for sexual purposes.

(ii) *Co-operation with law enforcement:*

(A) All ISPs must be made aware of their obligations in the face of a request by law enforcement for subscriber or data traffic information.

(B) All ISPs should be informed of the voluntary efforts they can engage in to assist law enforcement and to keep their facilities clear of child pornography.

(1) Model Acceptable Use Policies (AUPs) should be developed and disseminated which set out the range of voluntary measures ISPs can take which do not expose ISPs to liability under either privacy or other regulatory obligations.

(c) <u>Legislative reform</u>:

ISPs are major players in the Internet community. As all Internet traffic means business for them, a "blind eye" approach is tempting. Realizing their unique ability to assist law enforcement, some companies and industry associations have demonstrated leadership to help reduce the trade in child pornography over their networks and servers. However, some companies which have been quietly co-operative are reluctant to publicize their efforts to assist law enforcement for fear of backlash from subscribers. Therefore:

(i) ISPs should be required to disable access to child exploitation materials upon receiving notice from a designated law enforcement entity.

(ii) ISPs should be required to report child exploitation materials encountered on their facilities.

(d) <u>Incentives for development of technical tools</u>:

Law enforcement needs sophisticated tools to combat online child exploitation. However, private industry does not generally view this as a lucrative area in which to invest. Microsoft Canada's development of CETS in collaboration with law enforcement is a shining exception. However, to encourage more companies to invest in development of technical tools:

(i) Incentive programs, whether in the form of grants to university researchers or tax rebates to businesses, should be established to encourage the development of forensic software tools for use by law enforcement.

Educating Young People and the Public

Education is a crucial component of any preventative and enforcement strategy. The following recommendations address specific populations that should be addressed by educational programs. Focus group studies of young people, teachers and computer technicians in high schools should be funded in order to insure that the needs of the youth population are accurately being met.

(a) Educating children:

Children 12 and under usually become victims of online child exploitation in the course of offline abuse. Therefore:

(i) Educational initiatives aimed at empowering children to recognize and report abuse should include information about inappropriate picture and video taking.

(ii) Children should be informed of resources for reporting negative online (and offline) experiences, including cybertip.ca and Kids Help Phone.

(b) Educating adolescents:

Young people over 12 are often, though clearly not always, complicit in their own exploitation, both in the context of online meeting crimes and child pornography production. Therefore:

(i) Studies should be funded to learn from young people themselves what makes them susceptible to sexual relationships with adults, and what makes them willing to take sexual pictures of themselves or allow others to take such pictures of them.

(ii) Surveys should also be conducted with teachers and technicians responsible for computers in high schools. These teachers and technicians have insights into the materials that young people access via the Internet.

(iii) The results of these studies should be used to devise educational programs about the emotional and developmental dangers of engaging in these behaviours. Effective methods for conveying such information to adolescents include:

(A) Peer educators and student ambassadors who go into classrooms to discuss their negative experiences with other students.

(B) Multi-media workshops which students can complete individually and privately.

(C) Curriculum guides for use in health and sex education classes in high schools.

(iv) This initiative should be publicized via a visible event showcasing the involvement of youth in developing the materials.

(c) Educating parents:

Parents are often not as sophisticated as their children and teenagers when it comes to Internet use. Therefore:

(i) Educational materials for parents should be available through both online and more traditional channels, like print publications and community meetings.

(ii) Parents should be made aware of the possible complicity of their young teenage children in these sexual behaviours, and be on the lookout for them.

(iii) Parents should also be cautioned about putting pictures of their children online, as these can be morphed onto existing child pornography in order to produce images featuring new faces.

(d) Educating the public:

While often in the news, there are still widespread misconceptions about what child pornography offences are, and what activities online incur criminal liability. Therefore:

(i) A government sponsored online resource should provide information to the public about what child pornography is, and what online activities are illegal with respect to child pornography.

(ii) This resource should also instruct the public about how to report child pornography encountered accidentally, either through a virus or through file sharing activities, without incurring criminal liability.

(iii) Reporting resources like cybertip.ca should be widely promoted, including through the help of ISPs and computer software and hardware retailers.

We are all part of the Internet community. Purging child exploitation from the Internet is a mutual project, shared by law enforcement, the ISP industry, and the public. The foregoing recommendations for policy and legislative reform are offered in the spirit of this shared responsibility.

PART ONE: INTRODUCTION

When Michael Briere pleaded guilty to the 2003 rape and murder of 10-year-old Holly Jones in Toronto last year, he claimed he had viewed child pornography over the Internet just before the crime. The statements sparked nationwide calls to step up efforts to suppress the traffic in child pornography over the Internet, and has led to sustained attention to the problem by the media, police and politicians. While this little girl's death is by no means a typical outcome of the trade in child pornography, it represents an extreme consequence of a trade that necessarily involves the sexual abuse of children. And by the accounts of law enforcement officers and researchers working in this field, the ease of finding like-minded people and reduced fear of exposure made possible by the Internet has made this a growing problem, with a constant stream of new images appearing, and with images of younger children subjected to gross sexual assaults becoming more and more common.[3] Further, studies show that among Internet-related crimes with juvenile victims, production of child pornography, whether or not for distribution, is a common feature.[4]

A second type of sexual exploitation involving the Internet arises out of one of the Internet's many positive characteristics: through applications like chatrooms and instant messaging, making social contacts online has become easier and in most cases has enriched the lives of participants. But the meeting places of the Internet are also ripe for the exploitation of young people's emotional needs and sexual curiosities by adults. Child "luring" or, more accurately, crimes involving adults meeting young people for sexual purposes, have also garnered a significant degree of attention from the media, police and government, partly because these crimes tap into the fear that even when a child is safely within the confines of home, an

[3] Studies on the correlation between child pornography offences and contact offences vary, and many scholars caution that because of the fact that it is not known how many people possess child pornography accurate statistics are not possible. See the ISOCE presentation of Ethel Quayle, COPINE Project, University College, Cork, available at http://www.innovationlaw.org/pages/child_docs/Quayle.ppt. Some studies place the correlation as high as 76%. However, the US Postal Inspection Service found that nearly 40% of the offenders who were originally investigated only for child pornography had molested children. See the ISOCE presentation of Drew Oosterbaan, Chief, Child Exploitation and Obscenity Section, available at http://www.innovationlaw.org/pages/child_docs/Oosterbaan.ppt.

[4] In the Crimes Against Children Research Center's National Juvenile Online Victimization Study, a survey of U.S. law enforcement agencies' arrests for Internet-related crimes with juvenile victims, one quarter of online meeting cases and half of other crimes involved pornography production featuring the victim. See the ISOCE presentation of Janis Wolak, Crimes Against Children Research Center, available at http://www.innovationlaw.org/pages/child_docs/Wolak.ppt.

Internet-linked computer can lead a young person into emotionally or physically dangerous encounters.

There are many initiatives already underway in Canada and within the provinces which aim to address these problems, including the federal working group consisting of members of law enforcement, government and Internet Service Providers, the national Internet hotline cybertip.ca run by Child Find Manitoba, the National Child Exploitation Coordination Centre, and the Ontario Attorney General’s Working Group on Internet Crimes Against Kids. Canada is also participating in international efforts like the Virtual Global Taskforce, and is working toward ratifying international treaties that address these crimes. These recommendations are offered in an effort to assist and augment the work of these groups and institutions.

In particular, we aim to suggest approaches to these problems from multiple fronts, treating them as public health problems, requiring preventative measures as well as effective eradication measures. Misconceptions of the dynamics of these crimes lead to misplaced attention and resources in the face of a situation where more and better targeted resources are badly needed. Further, we suggest that all solutions offered must balance fundamental rights like freedom of expression and privacy with the need to protect children from exploitation, and suggest that there are ways of finding solutions that do not compromise any of these important values. All solutions suggested in this paper should be implemented in consultation with the Privacy Commissioner, and with a view to protecting fundamental rights while protecting children and young people from harm. Further, we offer these solutions exclusively in the service of reducing the incidence of online child exploitation and do not endorse any of our suggestions as applied to other criminal or civil offences.

Internet users and suppliers need to help serve the community in cyberspace. We therefore encourage partnerships with industry and with members of the public to see the project of protecting children from exploitation online as a shared project requiring shared responsibility, and applaud efforts already underway to this end.

PART TWO: PREVENTION STRATEGIES: EDUCATING YOUNG PEOPLE AND THE PUBLIC

Education is an important component of any preventative and enforcement strategy, and we praise the efforts of programs like Be Web Aware to educate children, parents and teachers about safe use of the Internet. We offer these suggestions as to areas where further efforts are necessary to accurately address the dynamics of both child meeting and child pornography crimes.

II. 1. *Education of Children and Adolescents*

Research presented at the ISOCE concluded that children under 12 are differently situated in relation to sexual exploitation crimes committed over the Internet than young people between 12 and 15. Efforts to educate children under 12 about the dangers of meeting with someone they met online, for instance, continue to be appropriate. However, the vast majority of meetings with adults initiated online involve young people between the ages of 13 and 15. Further, child pornography featuring children under 12 is typically produced in the context of classical offline child abuse. That is, children abused by family members, close family friends, or caretakers. By contrast, child pornography featuring children over 12 is often (though clearly not always) produced in the context of consensual or quasi-consensual relationships.[5]

II. 1.a. *Children 12 and under:*

As most child pornography featuring younger children is produced in intrafamilial abuse contexts, children in abusive family situations are particularly at risk of being exploited in this additional way. We recommend that educational programs that aim to empower children to recognize and report abuse should include education on inappropriate picture and video taking. Since sexual picture-taking is frequently a prelude to escalated abuse, children should be taught to recognize that photography and videomaking involving sexual organs or suggestive posing is an activity that should be reported to a trusted adult outside the context in which the pictures are being taken.

[5] See the ISOCE presentation of Janis Wolak, supra.

Children under 12 should be made aware of resources for reporting and discussing negative experiences, both online and offline.[6] Both cybertip.ca and Kids Help Phone (which has an online as well as telephone counselling component) are valuable resources for children who are victims of abuse, who are propositioned in chat rooms or who have unwanted sexual images sent to them. Kids Help Phone is particularly valuable for discussing abuse experiences, since the service offers trained counsellors and is anonymous.

II. 1.b. *Young people ages 13 and older:*

The same empowerment messages and information about reporting and counselling resources should also be part of programs aimed at young people 13 and over. However, the experiences of young teens, both online and offline will likely be different than those of younger children and so require additional content. Materials directed at teens should address situations which the teen may not think of as abusive but which are nonetheless exploitative and which are likely to have negative emotional and developmental consequences.

Research shows that contrary to popular belief, most online meetings between adults and young people for sexual purposes do not involve deception as to the age of the perpetrator or deception regarding whether the perpetrator is interested in sex.[7] Instead, young people are typically courted by an adult, generally a man over the age of 25, who showers compliments and gifts on the young person so that by the time the meeting takes place the young person believes he or she is involved in a romance. The young person agrees to meet the adult knowing both that

[6] According to the Youth Internet Safety Survey, 1 in 5 children aged 10-17 have received unwanted sexual solicitations online. See the ISOCE presentation of Drew Oosterbaan, supra.

[7] See ISOCE presentation by David Finkelhor, Director, Crimes Against Children Research Center, University of New Hampshire, regarding the National Juvenile Online Victimization Study conducted by the CCRC, available at http://www.innovationlaw.org/pages/child_docs/Finkelhor.ppt. See also David Finkelhor, Janis Wolak and Kimberly Mitchell, "Internet Initiated Sex Crimes Against Minors: Implications for Prevention based on Findings from a National Study," *Journal of Adolescent Health* 2004, available at http://www.innovationlaw.org/pages/child_docs/CV71.pdf. In this study of nearly 500 arrests involving juvenile victims of Internet-initiated offences, only 1% of victims where 12 and none under 12. 26% were age 13, 23% age 14, 27% age 15, 14% age 16 and 8% age 17. 75% were girls, 25% boys. 76% were initiated in chatrooms. Only 1% of offenders were 17 or younger, 23% were 18-25, 41% 26-39, and 35% 40 or older. 70% of offenders did not lie about there age at all and a further 25% shaved off a few years but still presented themselves as older adults. Only 5% presented themselves as minors. 80% openly brought up sexual topics with the victim. Often the courtship went on for a month or more before a meeting, which took place in 74% of the cases. Where face-to-face meetings occurred, 93% involved sexual contact, and 73% met more than once. 59% of female victims and 25% of male victims felt love or close friendship with the offender. Only 5% involved violence or force.

he is significantly older and that he wants to have sex. The deception typically lies in the promise of romance, not in the sexual nature of the meeting.

More attention needs to be paid to educating the 13-15 year old age group about the problems associated with meeting adults online, and in general about engaging in sexual relationships with adults, whether romantic or not. Funding should be made available to sponsor studies of these issues through talking to young people themselves, in an effort to both understand what young people think and feel about romantic and sexual relationships with adults and what makes them susceptible to them. We suggest that a project should be initiated featuring focus groups of young people, especially young girls and gay youth, in order to determine strategies that will work to educate these groups about the drawbacks of having sex with adults. These strategies should, for instance, address the emotional consequences of realizing you've been used, or of later regretting having experienced early sexual encounters in that context.

A further feature of the study should be a discussion with teachers and technicians in high schools who are responsible for maintaining high school computer systems. These teachers and technicians have knowledge of some of the illicit activities that students in this age group engage in, as they regularly encounter traces of these activities on school computers.

The 13 and over age group also experiences victimization by child pornography differently than younger children. Young people often, though clearly not always, voluntarily participate in their own exploitation by willingly posing for pictures or even taking the pictures or videos of themselves engaged in sexual poses or acts. Young people in this age group therefore have to be explicitly educated about the consequences of taking sexual pictures of themselves or letting someone else take sexual pictures of them. Young people must be made aware of the fact that images that make their way onto the Internet essentially "never die" and are circulated for decades among thousands of collectors. The education process here will surely need to address the larger issue of why young people, especially young girls, are susceptible to the flattery which convinces them to take such photos, and the larger cultural context which currently everywhere features young women in sexualized ways. Young teen girls are routinely sexualized in the media, and teenage girls need to be encouraged to find more positive self-affirming ways of feeling good about themselves, making them less susceptible to wily adults who prey on their insecurities.

Specific focus groups should also be conducted with gay male youth. As many gay youths will not be willing to openly acknowledge their involvement with adults online, educational materials will need to be developed which are sensitive to these confidentiality issues. Gay male youth may find meeting adult men online to be an accessible means of exploring their sexuality outside of the critical eye of peer groups. These feelings should be acknowledged in the materials. However, the long term consequences of allowing photographs or videos to be made, in particular the chance that they will make their way onto the Internet, must be addressed with this group of young people as well.

We acknowledge that educational efforts in this area will be challenging, since teens may be unreceptive to the message. Models for educating young people that have worked in other areas, like drug, alcohol, and tobacco awareness programs should be utilized. Young people are receptive to peer educators and student ambassadors who go into classrooms, and in this context such a program should feature young adults who were victims to this type of manipulation and only later regretted having had sexual relationships with adults, or young adults who only later regretted having sexual pictures of themselves circulated over the Internet.

Curriculum guides for use in health and sex education classes should accompany such a program. Multimedia programs should be developed where students can explore their personal feelings, experiences and knowledge of these activities individually and confidentially. The program should again feature information about the availability of anonymous counselling services for young people, like Kids Help Phone, where a young person can go to discuss experiences, via telephone or Internet, which have left them hurt or confused. As noted above, young people should also be made aware of the existence of cybertip.ca as a place to report negative Internet experiences, bearing in mind that young people may not experience the encounter itself as negative until a later date, after the “relationship” with the adult goes sour.

Since some students may feel more comfortable learning about these subjects outside of school, Internet service and Internet content providers who provide services and/or content to young people should be encouraged to include a version of these materials on their teen oriented web pages.

This educational initiative should be launched via a visible event showcasing the entire youth consultation process. Such a strategy will help ensure that young people feel involved and so are more likely to listen to the message being conveyed.

II. 2. *Education of parents*

Young people are often more technologically sophisticated than their parents. Therefore, any educational materials or programs for parents should include more traditional modes of address, including print publications and in-person information sessions at community meeting places.

Parents should be made aware of the dynamics of online meetings between adults and young teens. Specifically, parents should be made aware that young teens are often complicit in meeting the adult who has romanced them online, and often meet the adult more than once. Parents can help to educate their children about the hazards of meeting someone who appears to be nice to them, both online and offline.

Parents should be cautious about putting pictures of their children online, especially together with identifying information. Further, parents should also be made aware that new and easily accessible technologies make it possible to produce "morphed" sexual abuse images, by taking innocuous pictures of children and grafting them onto existing child pornography.[8]

Parents should be made aware of the existence of cybertip.ca to report incidents they become aware of where their children have been propositioned or sent inappropriate material online.

II. 3. *Education of the public in general*

Child pornography is often in the news, yet there are many misconceptions about what it is and what it isn't. An online resource should be established, most likely through the Department of Justice, which provides information to the public about the legal definition of child pornography, about precisely what online activities are illegal (i.e. accessing, downloading, transmitting child pornography online), and the various statutory offences involved in having sexual relations with a minor. Further, since most child pornography production cases come to light by way of citizen reports (either through victim disclosure, someone finding pictures, suspicions of family or community members), mechanisms for reporting offline abuse should be part of the campaign.[9] Indeed any public education campaigns on these topics should include

[8] See the ISOCE presentation of Jane Bailey, University of Ottawa, Faculty of Law Common Law Section, available at http://www.innovationlaw.org/pages/child_docs/Bailey.ppt.

[9] Studies indicate that the majority of child pornography production cases, perhaps as high as 91%, come to light through citizen reports, rather than through online investigation. See the ISOCE presentation of Janis Wolak, supra.

both online and offline components, so as to address the broader population that is less computer savvy as well.

The resource could also address common fears and misconceptions about “accidental” possession of child pornography, for instance fears of getting child pornography on your computer via a virus or other malicious code, or by downloading a seemingly innocuous file via a peer-to-peer service that turns out to have been misleadingly labelled. The resource should instruct the public what they should do when they encounter child pornography online, and instruct them on how to report this material without incurring criminal liability themselves. This resource would also be useful to Internet Service Providers (ISPs), which could refer subscribers to the resource via embedded links in their Acceptable Use Policies.

As noted above, we consider cybertip.ca and Kids Help Phone to be valuable resources, and suggest that ISPs should be approached about the possibility of including shortcuts to these services as part of their Internet Access software. We further suggest that computer hardware manufacturers and/or retailers should help distribute brochures or leaflets about these services with computer hardware purchases.

PART THREE: ENFORCEMENT STRATEGIES: RESOURCES AND TRAINING FOR POLICE AND PROSECUTORIAL SERVICES

We applaud the great strides made in creating specialized police units to deal with Internet crime, and in particular to deal with the sexual exploitation of children using the Internet. These specialized units should continue to be promoted, and will need increased funding to be able to keep up with the technological sophistication of perpetrators.

III. 1. *Police training re online meeting crimes*

Research indicates that one area where police training and culture can be improved is in the handling of statutory sexual offences committed over the Internet. As discussed above, these crimes often involve a complicit young teenage victim. Police services need to be educated as to the psychology of young adolescent girls and gay youth, who may feel affection towards the adult with whom they have been having sexual relations. Youth advocates and peer support programs should be in place for these victims, which can specifically address the complex emotional issues often involved for the young people exploited by these crimes.

III 2. *Police training re child pornography*

Research indicates that the majority of child pornography, especially that involving younger children, is produced within traditional abuse contexts, namely perpetrated by family members or close acquaintances, and so connections between high technology units and more general sex crimes or child protection units are vital. Officers working in the area of child abuse should also be aware that child pornography production may be a part of the abuse behaviour and be prepared to investigate this possibility in every case.

There is some evidence that young offenders are increasingly represented among those charged with child pornography crimes. These offenders should be handled differently than adult offenders, in that some research indicates that the use of child pornography is a sign of other problems faced by the young person. Young people with problems may turn to collecting child pornography due to the ease of access that the Internet affords, exacerbating other poor coping mechanisms.[10] Use of child pornography by a young person should be seen as a child

[10] Studies show that young people are often exposed to sexual material online and that viewing pornography online can become addictive as a way to assuage emotional distress. See the ISOCE presentation of Ethel Quayle, supra.

protection issue for both the victim of the images and for the young person charged with possession or distribution of such images.

III. 3. *Special prosecutors*

We suggest that Canada should consider following the model in other jurisdictions wherein specialized prosecutorial services have been successfully established to deal with Internet related crime.[11] Due to the technical nature of the evidence, Crown prosecutors with experience in handling these types of cases have an advantage over inexperienced Crown counsel, and should be better able to make the evidence comprehensible to members of the judiciary who may not have encountered these crimes before.

III. 4. *Collaboration with industry*

We applaud efforts to bring together police services, Crown prosecutors and representatives from the ISP industry. These efforts should continue, and be supplemented by discussions between police services and software and hardware developers. The industry representatives have valuable knowledge to impart to the police services, and police services are able to inform industry of the misuse of their products in ways that help encourage technological or business-model solutions.

[11] See the ISOCE presentation of Drew Oosterbaan, supra.

PART FOUR: THE ROLE OF INTERNET SERVICE PROVIDERS AND RELATED INDUSTRIES

We recognize the efforts that the industry associations, the Canadian Association of Internet Providers (CAIP) and the Canadian Cable Television Association (CCTA), have made to date in finding collaborative solutions to making police investigations of online child exploitation crimes more effective. We also recognize the industry's need to guard the privacy of its subscribers, and so to ensure that disclosure of subscriber information only occurs under proper circumstances. However, we suggest that online child exploitation is an especially heinous type of online crime, and therefore requires stronger measures than other types of online problems, such as those that involve threats to financial interests (phishing, fraud, hacking, intellectual property infringement). We would therefore restrict the following suggestions to ways of dealing with online child exploitation, and do not see these recommendations as extending to other types of illegal activity online.

IV. 1. *Encouraging effective self-regulation*

Effective self-regulation has been a central tenet of Canadian policy toward new media from the beginning.[12] Large industry players have been generally responsive to the need to take action to help decrease the incidence of child exploitation crimes. However, there are many smaller ISPs who have not been centrally involved in the discussions with government and police services, and so continue to be unaware of the role they can play. Stronger measures should be taken to raise awareness among all members of the Industry regarding steps they can and should take to help reduce the incidence of these crimes.

An effective means of communicating with a large number of industry members is through the industry associations. However, not all ISPs are members of these associations. Mandatory membership in industry associations would insure that all ISPs can be reached, but it is an unpopular solution among members of the industry. Other measures for reaching ISPs who are not members of these associations should therefore be undertaken, for instance through mailings to lists specifically compiled for this purpose, which could be gleaned from Internet resources by a research assistant under contract to the Department of Justice. Alternatively,

[12] See the ISOCE presentation of Andrea Slane, Centre for Innovation Law and Policy, University of Toronto, available at http://www.innovationlaw.org/pages/child_docs/Slane.ppt.

CAIP and CCTA could be encouraged to compile lists of non-members, if they do not already do so, which could also serve as a mailing list for our purposes. Finally, provincial ministries of business services could send out mailings to all businesses registering names which contain words implying Internet services, such as “net”, “web”, and “online”.

IV. 2. *Raising awareness among ISPs of the measures they can take to help reduce these crimes*

IV. 2. a. Education of subscribers

ISPs are in a position to provide their subscribers with information about Internet safety, especially for parents, children and adolescents. While large service providers often have this type of information on their websites, smaller service providers are less likely to do so. Small service providers should therefore be provided with guidance as to how to impart such information to subscribers, either via their own websites or by referring subscribers to other resources (for instance, the Be Web Aware website). This guidance can be disseminated either via ISP associations or through mailings from the ministries responsible for business name registrations.

We further suggest that all Canadian Internet users should be made aware of the existence of cybertip.ca. Again, ISPs can play a key role in informing their subscribers, provided that all ISPs are aware of the tip line and its purpose.

ISPs are also in a position to provide education to their subscribers as to what sorts of behaviours are illegal online. Currently, this information is often conveyed via the listing of activities which will not be tolerated by the service provider, usually within Acceptable Use Policies (AUPs).[13] As discussed above under “Education of Young People and the Public”, a government supported resource should be developed which explains what sorts of content constitutes child pornography and what sorts activities are illegal (i.e. downloading, transmitting, sharing, accessing). ISPs could direct their subscribers to this resource in the context of their AUPs, or wherever else Internet safety issues are discussed on their websites.

[13] See the ISOCE presentation of Andrea Slane, supra.

IV. 2. b. Legal parameters of privacy obligations and voluntary measures for co-operation with police

Large ISPs are well aware of their obligations in the face of a court order for subscriber information. Smaller ISPs may not be as informed of their obligations and should be educated about them. Especially in light of the development of a new form designed to facilitate the process of obtaining the production of basic subscriber information in child pornography investigations, an industry-wide education effort needs to occur, both within the ISP industry associations and in such a way as to reach those businesses that are not members of these associations, as suggested above.

In terms of voluntary measures, it is already common practice among several large ISPs to state that where child pornography is found on their networks and servers, police will be notified. Further, while not wanting to be obligated to routinely monitor their networks and servers, many ISPs reserve the right to occasionally monitor the content and traffic information on their facilities for the purpose of enforcing their AUPs. We encourage the development of model user agreements and model AUPs which elevate the industry's ability to assist law enforcement while protecting these companies from liability under federal and provincial privacy legislation, or any other applicable telecommunications regulations.[14] These models would have the benefit of insuring that those ISPs that use them would comply with the legal constraints on disclosure of subscriber information, while clarifying what level of internal monitoring an ISP can engage in. As these are contractual matters between ISPs and subscribers, it should again be stressed that this level of co-operation can be confined to this type of crime only, and should remain voluntary for ISPs.

IV. 3. *Legislative measures to consider*

IV. 3. a. Notice and takedown

We acknowledge that ISPs are generally cooperative and voluntarily take down child exploitation materials housed on their facilities once they become aware of them. However, we suggest that a regime should be established where Canadian ISPs are required to take down child exploitation material housed on their facilities upon receiving notice from law enforcement, and

[14] See the ISOCE presentation of Andrea Slane, supra.

that upon such notice an ISP should further be required to retain whatever records they have in connection with that material for inspection by police once the proper order is served. This would ensure the timely retention of records and allow police services the time needed to get the appropriate order. A copy of the European Union E-Commerce Directive, which contemplates such requirements, is available at Appendix C.[15]

We note that the Australian regime allows the entity to which the public reports child pornography, the Australian Broadcasting Authority (ABA), to issue take-down notices for Australian hosted material. Since the tip line in Canada is run by an NGO, cybertip.ca, the authority to issue such notices will likely have to be once removed from the front line reporting process. We suggest that as cybertip.ca vets complaints and determines which ones are to be forwarded to law enforcement, that a national law enforcement entity should at this point be authorized to issue take-down and/or data retention notices to ISPs for Canadian hosted materials, that is, simultaneous to sending complaint information to local law enforcement jurisdictions. A copy of the Australian legislation is available at Appendix D.[16]

As with all suggestions so far, we again stress that we draw a distinction between child exploitation content and other types of illegal content, especially copyright infringement which we see as a separate issue entirely.

IV. 3. b. Reporting requirements

We suggest that where ISPs come across child pornography in the course of ordinary business, that they should be under a legal obligation to report that material and its location to a designated police contact. The U.S. has a reporting requirement wherein ISPs are obligated to

[15] We note that the European Community E-Commerce Directive (Directive 2000/31/EC) states at Article 40 that "service providers have a duty to act, under certain circumstances, with a view to preventing or stopping illegal activities; this Directive should constitute the appropriate basis for the development of rapid and reliable procedures for removing and disabling access to illegal information; such mechanisms could be developed on the basis of voluntary agreements between all parties concerned and should be encouraged by Member States", and at Article 46 that "In order to benefit from a limitation of liability, the provider of an information society service, consisting of the storage of information, upon obtaining actual knowledge or awareness of illegal activities has to act expeditiously to remove or disable access to the information concerned". See the ISOCE presentation of Frédéric Mégret, University of Toronto, Faculty of Law, available at http://www.innovationlaw.org/pages/child_docs/Megret.ppt; Appendix C is available at http://www.innovationlaw.org/English/Child-Exploitation-Appendices.html.

[16] See the ISOCE presentation of Tony Krone, Australian Institute of Criminology, available at http://www.innovationlaw.org/pages/child_docs/Krone.ppt. The Broadcasting Services Amendment (Online Services) Bill 1999 is available at Appendix D, which is available at http://www.innovationlaw.org/English/Child-Exploitation-Appendices.html.

report such material to the national tip line, which then issues a receipt which serves to protect the ISP from liability.[17] We suggest that cybertip.ca could issue such receipts, although again the propriety of having an NGO serve such a function should be considered.

We note that Australia has recently created a new telecommunications offence, which requires ISPs and Internet Content Hosts to report child abuse material which they are aware can be accessed using their service to federal police under a $10,000 penalty for failure to report.[18] We attach a copy of the U.S. and Australian legislation at Appendices E and F, respectively.[19]

Such a reporting requirement would alleviate the need for ISPs to justify reporting to subscribers, and specific parameters of the reporting requirement should be worked out with the Privacy Commissioner. The reporting requirement should be linked to reporting requirements already in place for social workers, therapists and others who work with children, in order to stress the fiduciary responsibility involved in protecting children from further harm.

In suggesting a reporting requirement we do not suggest that ISPs should be under an obligation to actively patrol their networks. The requirement would only arise where material is found in the normal course of their business activities.

IV. 4. *Incentives for development of technological tools*

Combating online child exploitation requires sophisticated technological tools. However, because the market incentives for investing in the development of tools that effectively block, detect or track known child pornography images are weak, an incentive program should be established that encourages such development. Such incentive programs could include grants to academic researchers, or tax incentives for private enterprises.

A similar incentive program should be established to encourage software developers to develop forensic tools to assist police. Software assisted forensic analysis of child pornography collections, for instance analysis of a suspect’s hard drive for known child pornography images via digital hash values, greatly increases the effectiveness of police investigations and evidence gathering. We commend the voluntary contributions of the software industry on this count,

[17] 42 U.S.C. § 13032. See the ISOCE presentation of Drew Oosterbaan, supra.

[18] *Crimes Legislation Amendment (Telecommunications Offences and Other Measures) Bill (No. 2) 2004,* s. 474.25. See the ISOCE presentation of Tony Krone, Australian Institute of Criminology, supra.

[19] The appendices are available online at http://www.innovationlaw.org/English/Child-Exploitation-Appendices.html.

especially Microsoft Canada's development of the Child Exploitation Tracking System (CETS). However, such extraordinary voluntary efforts are rare and so private investment in these types of products should be more actively encouraged.

Before the system-wide implementation of technological measures occurs, extensive collaborative study between government and the ISP industry will be necessary, in order to assess the technological and economic impact of such measures on both quality of service and the competitiveness of the Canadian ISP industry. Further, while we acknowledge that technologies that block access to known child pornography have both benefits and risks, including potentially squeezing supply enough to encourage an increase in new production, we feel the benefits to limiting access to known child pornography images should weigh in favour of supporting such solutions. However, frequent assessment of the impact of these technologies on the production of child pornography should be part of any implementation scheme.

PART FIVE: TOWARDS INTERNATIONAL HARMONIZATION

As online child pornography crimes often involve international transmission of prohibited material, participation in international investigations is standard practice and Canada has been at the forefront of international co-policing efforts. However, while we recognize the need to progress toward ratification of international instruments like the Cybercrime Treaty with care and deliberation, so as not to compromise fundamental Charter rights, we feel that there are some aspects of the online child exploitation problem that can be dealt with more expeditiously in order to bring Canada in line with its international obligations.

V. 1. *Consolidation of databases*

We endorse the value of consolidating databases containing known child pornography images and their digital hash values. In the Interpol investigation Operation Enea, for instance, Norwegian and Danish police searched shared folders on peer-to-peer networks using known hash values and found nearly 1300 IP Addresses with 7 or more matches in the U.S. alone.[20] We encourage the development of a Canadian central database, which can be linked to international databases as they are established. Such databases should be searchable by hash value in order to assist police in analyzing files seized from the computer of a suspect, so as to save valuable resources otherwise expended on opening and reviewing each of thousands of digital image files. As noted above, development of appropriate software goes hand in hand with the establishment of such databases.

We suggest that these databases should be subdivided so that images depicting identified victims are contained in a sub-database, so that efforts to identify such victims can be globally discontinued. To illustrate, we note recent massive efforts to rescue a young girl depicted in a series of pornographic images, involving both Canadian and Florida police. After releasing photos to the public containing clues to the identity of the victim, information from one of the several U.S. national databases indicated that the girl had already been rescued two years earlier and her abuser was already serving time in prison for his crimes. Further, two of four claimed success stories where perpetrators pictured in child pornography were identified through tips on the television program America’s Most Wanted actually involved people who had already been

[20] See the ISOCE presentation of Drew Oosterbaan, supra.

convicted and were serving time in prison for child pornography or child abuse related crimes.[21] While these are happy outcomes, it should not take so long, and hence so many resources, to determine that a perpetrator has already been captured and a child identified and saved from further harm.

V. 2. *Mutual Legal Assistance Treaties*

The Mutual Legal Assistance Treaties (MLATs) allow evidence gathered in foreign jurisdictions to be used in Canadian courts. These treaties are outdated, however, because they do not deal with the exigencies of electronic data evidence. Canada should take the lead in updating these treaties in order to make them able to accommodate the use of data traffic logs, chat room logs, e-mail attachments, shared file directories and so forth which have been obtained with the help of foreign law enforcement services to be used in Canadian courts.

V.3. *Investigative information sharing*

International information sharing at the investigative stage, for example through the Child Exploitation Tracking System (CETS), likewise needs proactive attention by Canada and other national governments. As the first national host of CETS, a data sharing tool developed jointly by Microsoft Canada, the Royal Canadian Mounted Police and Toronto Police Services, Canada is well placed to show leadership by forging the legal instruments necessary to allow functional investigative information sharing internationally, which could then serve as a model for other nations.

V. 4. *Sentencing*

Participants noted that the sentences handed down in child pornography cases in Canada are generally too low, especially as compared to other jurisdictions, indicating that the judiciary needs more guidance on the seriousness of these crimes. The European Framework Decision, for instance, specifies that penalties will normally be between one and three years, and five to ten years for aggravated offences.[22] In the U.S., the *Protect Act of 2003* provides for stiff penalties

[21] See the America's Most Wanted website, at www.amw.com.

[22] Aggravated offences include where the child is below the age of consent, where the offender has endangered the child's life, where the offence involved violence or caused serious harm to the child, and where the offences are committed in the context of a criminal organization. See the ISOCE presentation of Frédéric Mégret, supra.

upon conviction for a second sexual offence involving a minor, including child pornography offences, and the possibility of supervised release for life for child pornography offences. A copy of the legislation is available at Appendix G.[23] We suggest that sentencing guidelines be established which stress that the mandatory minimums recently set for select child exploitation crimes in Bill C-2, which received Royal Assent on July 20, 2005, are the low end of the sentencing scale for child pornography crimes. The judiciary should be encouraged to send the message that all child pornography offences are serious offences that participate in the abuse of children.

V. 5. *Statutory Sexual Offences*

As discussed under the heading “Educating Young People and the Public” above, research indicates that the group most vulnerable to being seduced by an adult online is young adolescents between the ages of 13 and 15. This same research indicates that most offenders are over 25 years of age.

We support the general project undertaken in the newly enacted amendments to the Criminal Code found in Bill C-2, which aim to protect young people by adding the category of “exploitative” relationships to the category of prohibited relationships with young people over 14. However, we are concerned that the concept of exploitation may not capture relationships where an adult has seduced a young person with promises of love and romance, when the aim of the relationship for the adult is merely to engage in sexual relations. We are concerned that the young person might be invested in perceiving the relationship as a romance and so might not immediately perceive these relationships as exploitative. Further, we recognize that manipulation of this sort is rather common among young people in peer relationships as well. We therefore suggest that some clarification be given in commentary to the new amendments to the Criminal Code ushered in by Bill C-2, which both explains that manipulation contributes to a finding of exploitation, and which further distinguishes between peer relationships and relationships where the perpetrator is an adult more than five years older than the young person.

We note that Australia has recently enacted a nationwide prohibition against grooming a child for sexual purposes via its federal telecommunications regime, and that one Australian state

[23] See the ISOCE presentation of Drew Oosterbaan, supra. The *Protect Act of 2003* and 18 U.S.C. § 2251 and 2252 are available at Appendix G, available at http://www.innovationlaw.org/English/Child-Exploitation-Appendices.html.

has a criminal offence against grooming.[24] We consider this option to be worthy of further study, and copies of the Australian legislation are available at Appendix F.[25]

[24] In data collected for a study of the first 25 suspects charged for online grooming under the Queensland criminal provision where investigators posed as girls aged 13-15 in online chatrooms, 72% of those charged were charged with procuring a child for a sexual purpose and 28% were charged with exposing a child to indecent material. See the ISOCE presentation of Tony Krone, Australian Institute of Criminology, supra.

[25] Appendix F is available online at http://www.innovationlaw.org/English/Child-Exploitation-Appendices.html. See especially s. 474.26.

CONCLUSIONS

We have identified several areas where government should dedicate further resources and attention in order to reduce the incidence of online child exploitation:

EDUCATION OF YOUNG PEOPLE AND THE PUBLIC

- **Education of children and adolescents**: Children must be empowered to report abuse: this remains the best means of curtailing child pornography. However, the particular dynamics of child pornography production involving young teens also needs to be addressed, via investment in focus group studies and the implementation of a youth-involved educational initiative which addresses why young people often voluntarily become involved in making sexual images of themselves. Further, this age group must also be more realistically addressed regarding the frequency with which young people consent to sexual relationships with adults they have met online.

- **Education of parents:** Educational materials for parents, available in both online and offline forms, should alert parents to the realities of online meeting crimes involving young teens, namely that teens may be complicit in these relationships. Parents need to be equipped with this knowledge in order to talk to their children about the hazards of forming these relationships.

- **Education of the public**: Misconceptions about the seriousness of child pornography crimes abound. Therefore, a government sponsored resource should be established to inform the public about what child pornography is and what online activities are illegal (i.e. accessing, downloading, transmitting). The resource should also inform the public about how they can report child pornography without incurring criminal liability. Resources like cybertip.ca and Kids Help Phone should be widely publicized, including by ISPs and by hardware manufacturers and retailers.

RESOURCES AND TRAINING FOR POLICE SERVICES and CROWNS

- **Police training:** Police should be made aware that child pornography production is becoming a common feature of child sexual abuse, and that child abuse investigations should be alert to the possibility of additional related child pornography crimes. Young offenders charged with child pornography crimes should be handled as likely needing intervention of their own, as use of child pornography by young people may be a child protection issue in its own right. Police should also receive training on how to deal with statutory sexual offences initiated online, in particular how to deal with young teenage victims who have been complicit in these crimes.

- **Specialized Crown prosecutors**: Given the success of specialized police units and the technical nature of the evidence in online child exploitation crimes, specialized prosecutorial services should be established, allowing prosecutors to build on their experience prosecuting these crimes.

- **Collaboration with industry:** Discussions and collaborations between industry and law enforcement should continue, and should be expanded to include the hardware and software development industries.

ENCOURAGING ACTIVE ROLE OF INTERNET SERVICE PROVIDERS AND RELATED INDUSTRIES

- **Encouragement of effective self-regulation of Internet Service Providers**: We support the work of industry associations, and believe that widespread membership in such organizations is an effective means to ensure more uniform levels of awareness within the industry of measures that can be taken to minimize online child exploitation crimes. However, since not all ISPs are members of such organizations, measures should be taken to reach those non-member ISPs via mailings to business addresses gleaned from lists specifically compiled for this purpose.

- **Raising awareness among ISPs of voluntary measures they can take:** All ISPs should be made aware of publicly available resources dealing with online child exploitation, including cybertip.ca. Model Acceptable Use Policies should be developed and made available to all ISPs which illustrate the degree of co-operation with law enforcement that is acceptable under privacy and other regulatory legislation.

- **Legislative measures to consider:** A notice and take-down regime should be established for child exploitation materials, where the notice can issue from a central entity authorized to receive the complete list of reports deemed by cybertip.ca to qualify for forwarding to law enforcement. Notice should trigger records retention requirements, which would then be subject to the usual court order procedures. ISPs should be required to report child exploitation materials found in the normal course of business on their facilities. Reporting receipts can be issued by cybertip.ca or the same government entity that would issue the take down notices.

- **Incentives for development of technological tools:** A financial incentive program should be established to encourage the development of technologies to detect, track and block access to child pornography, and that provide forensic analysis tools for law enforcement. However, system-wide implementation will require further collaborative study, by industry and government.

TOWARDS INTERNATIONAL HARMONIZATION

- **Databases**: A national Canadian database of known child pornography hash values should be established, as linked to international databases where available. Such a database should be subdivided so that images depicting known victims and/or perpetrators are easily identified by law enforcement, so as not to waste resources searching for an already captured perpetrator or rescuing an already rescued child.

- **Mutual Legal Assistance Treaties:** These treaties should be updated so as to clarify the standards by which electronic evidence obtained from foreign law enforcement services can be used in Canadian courts.

- **Investigative information sharing:** The legal instruments necessary to allow functional investigative information sharing internationally should be drafted, which could then serve as a model for other nations.

- **Sentencing:** Sentences for child exploitation crimes should be more severe. Sentencing guidelines which stress that newly set minimum sentences are the low end of the sentencing scale should be established in order to provide guidance to judges.

- **Statutory sexual offences**: the definition of exploitative relationships should be clarified or explained in commentary to the new amendments to the Criminal Code brought in by Bill C-2, with particular attention paid to the manipulation of young people via promises of love and romance.

We appreciate the opportunity to put forward these strategies for combating online child exploitation. We encourage government bodies to act on them.