Staying safely connected: Updated strategies for protecting children and youth from exploitation online

A project of the Microsoft Safe Computing Program

2007

PREAMBLE

The Centre for Innovation Law and Policy has coordinated the preparation of this white paper on strategies to reduce the incidence of online child exploitation, based upon the papers presented at the 2nd International Symposium on Online Child Exploitation (2nd ISOCE) held on May 7, 2007 at the University of Toronto, and a roundtable discussion held on May 8, 2007. The Center is grateful to the experts who participated in these events, each of whom is listed in Appendices A and B, respectively, to this report.

The 2nd ISOCE, like the first held in 2005, brought together experts from diverse disciplines and fields in order to come to a better understanding of the issues associated primarily with two problems: a) the online trade in child pornography images, and b) adults meeting young people online for sexual purposes. The Centre organized the 2nd ISOCE as a follow up to the first ISOCE, both of which formed a major part of the Microsoft Safe Computing Program, a project of the Centre.

As the organizer of these events, the Centre Executive Director oversaw the preparation of this summary report of the major concerns raised by participants, along with the ideas expressed for addressing them. Participants in the 2nd 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 2nd ISOCE and roundtable discussion appreciate the difficulty in effectively addressing these and other Internet related crimes that threaten the healthy development of personal and sexual identities for and by young people. We encourage those in a position to implement these recommendations to see them as a means to strengthen existing efforts, and we encourage evaluation of existing efforts in order to further identify gaps in means to address online child exploitation in its ever evolving forms. 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 can contribute to their development.

We are grateful to Vicky Kuek for her dedication to this project, and, in particular, as principal author of this report.

Andrea Slane, *Executive Director*
Centre for Innovation Law and Policy

Table of Contents

1 EXECUTIVE SUMMARY: RECOMMENDATIONS FOR REFORM

Approach of this white paper

This paper builds on the white paper that followed the First International Symposium on Online Child Exploitation in 2005 ("First Symposium") and which is appended at Appendix C. Work that has been undertaken in the intervening two years across the various sectors of social science research, education, law enforcement and law reform has contributed new insights and also shed light on new issues. These were discussed at the Second International Symposium on Online Child Exploitation ("Second Symposium") held at the University of Toronto in May 2007.

The approach of this white paper is to provide detailed recommendations with respect to the themes that have arisen either for the first time or have occurred again in the Second Symposium, and this white paper should be read together with the recommendations made in the first white paper.

As with the first white paper, none of the contributors to this paper should be assumed to endorse all of the individual recommendations made.

Summary of Recommendations

The scourge of child pornography has been aggravated by the abuse of Internet and other digital technologies. A recent report in the *National Post* suggests that the Internet is a "unique enabler of child-porn offenders",[1] an assessment which is supported by the findings of some researchers who participated in the Second Symposium. And yet Internet technologies are also playing an increasingly prominent role in the healthy sexual development of young people as well. Some of the Symposium participants highlighted the challenges facing educators and policy makers to balance the realities of online youth behaviours with measures that will protect children and youth from sexual exploitation. The recommendations made in the first white paper are still useful and pertinent to this end. We propose that a study be conducted to assess the progress made in the last five years in combating online child exploitation, insofar as possible, and in the meantime propose the following measures as a follow-up to the first recommendations.

A. Educating youth

While there is a growing body of resources to educate and raise youth awareness in relation to the potential dangers posed by the Internet, there is concern that these resources are not, for one reason or another, being accessed by at-risk youth. Further, the advent of the Internet requires that all users be mindful of the privacy and control of material that enters the Internet and of interactions with others that occur online. This is

[1] Allison Hanes and Joseph Brean, "Online obsessions" *National Post* October 20, 2007, available at http://www.canada.com/nationalpost/news/story.html?id=efd2ea85-b98d-4cab-8b42-7e6d2ac72011 (accessed on October 25, 2007)

particularly true of youth, who may not grasp the implications of making personal material available online. We offer the following recommendations in this regard:

1. *Target educational campaigns to at-risk youth and articulate the reality of online grooming and youth-on-youth exploitation*

Social science research suggests that while youth appear to be more savvy and aware of the risks posed by certain conduct on the Internet, some youth still engage in risky behaviour. As articulated in the first white paper, youth may be complicit in their own exploitation – an element that is augmented by the ease and anonymity afforded by the Internet. Online grooming is now an offence under the Criminal Code, and the reality of online-grooming should be made clear to youth, specifically at-risk youth. Further, exploitation is not limited to adult-on-youth exploitation, as youth-on-youth exploitation is not uncommon. We recommend that existing educational material be re-positioned such that at-risk youth recognise themselves as at-risk, be equipped to recognise the signals of potential harm and be equipped with strategies to avoid or extricate themselves from harmful situations.

2. *Educate youth to understand the concept of sexual identity and equip youth with strategies to manage and protect it*

The ease of replication and dissemination of material online highlights the importance of youth managing their identities, including their sexual identities. If youth understand the concept of protecting their identities and the implications of losing control of their identities, they would then be likely to be more receptive to making informed decisions to protect it. Such education could be integrated into school's sexual education curriculum and should include education on media literacy, the aim of which should be to acknowledge the role of the Internet in some young people's healthy sexual exploration and to distinguish this from unhealthy behaviour that puts young people at risk of exploitation.

B. Cyber-bullying and sexual exploitation

The Internet has enabled new manifestations of existing problems, and the growing incidence of cyber-bullying is an example of this kind of harm. This is of particular concern as initial research has identified that, for example, friends who know secrets about friends can leverage this knowledge for sexual content.

1. *Further research and multidisciplinary collaboration to enable legislative clarification and progress*

Cyber-bullying is still not yet a well-understood area and further research is required. This would likely include surveys and focus groups of children and youth. This research would benefit from a multi-disciplinary and collaborative approach. Empirical evidence

arising from such research would be invaluable for informing further legislation and education responses.

2. *Provide parents, teachers and other guardians with immediate "hands-on" responses to cyber-bullying.*

Cyber-bullying is currently a phenomenon that is causing children and youth harm. Parents, teachers and guardians are rarely the first port of call for victims of cyber-bullying and so may either be oblivious to the issue, or may be suspicious of it occurring, but feel powerless to assist. Parents, teachers and other guardians can implement both technical and behavioural responses to curb and minimise the incidence of cyber-bullying. The various levels of government, working together with researchers, can take the initiative by providing suggestions, guidelines and behaviours to look out for.

C. Legal reform

1. *Balance the approach taken by the current child-pornography provisions in the Criminal Code by uncoupling the "broad net" approach to offences from the punitive mandatory sentencing regime.*

Canada's Criminal Code adopts a broad-net approach to what constitutes a child pornography offence. When taken together with the punitive mandatory sentencing regime, the legislation may suffer a loss of credibility as it may be perceived to have a moral core, but dubious periphery, which includes images such as those depicting adolescents or young adults in sexual poses or engaged in lawful sexual activity; and creative works that are products of the imagination, including stories and paintings. Such a stance does not reflect the evolving nature of childhood. It therefore might be useful to uncouple these two approaches and to have, for example, a separate regime dealing with "youth exploitation images". These "youth exploitation images" could include images of youth engaged in legal sexual activity, and not be tied to the mandatory sentencing regime.

2. *Reconsider the law's focus on fixation and recording to address the existence of streaming technologies.*

It has been suggested that the Criminal Code's focus on fixation and recording might harm rather than help. Technology has sufficiently advanced such that child abuse can be watched online as it happens. The current focus on recording and fixation may not be helpful to address all of the uses that can be made of technology in producing and making available child pornography, in that it may not capture the harms committed by live online audiences who may not collect images per se.

3. *Legislate to allow victims of child pornography civil redress against offenders.*

Victims of online child exploitation offences should be enabled to seek civil redress for the harms suffered, particularly as these harms may continue well into the future. This

type of legislation has been enacted in at least one state in the United States (South Dakota). Where general torts of privacy invasion are available via provincial legislation, the availability of this cause of action to victims of child pornography should be clarified and publicized.

D. Risk assessment for tools for sentencing

1. Develop risk assessment tools for use in sentencing

Social science research should be used to create risk assessment tools that can aid judges in the sentencing process. The sentencing process is particularly important in child exploitation offences as this is the forum where the question of child pornography offenders re-offending as sexual offenders has to be addressed. Further, mental health issues must also be considered, and offenders may be more appropriately referred to mental health treatment rather than, or in addition to, imprisonment.

E. In addition to the national sex offenders' registry, implement a searchable registry of body parts and other identifiable characteristics.

1. Implement a searchable database of the notable features of sex offenders

Currently, Canada's sex offenders' registry allows only notes and an image of the offenders' faces. However, it would be useful in the investigation and coordination of law enforcement efforts in online child exploitation if there were a searchable registry of images of sex offenders' distinctive features such as scars and tattoos. The sex offenders' registry could then be usefully cross-referenced with a catalogue of identifying features of perpetrators found in child pornography images where faces are not visible. We recommend that a study of such a database be conducted which assesses the *Charter* viability of such a registry as a next step toward its implementation.

2 CONTEXT

It is clear that the online exploitation of children persists as a pernicious world-wide problem. This is supported by the work presented at the Second Symposium and the discussion generated by it, together with incidents reported in the general media. The seriousness of this abuse and its manifestation continue to escalate. According to Andrew Oosterbaan,[2] the nature of current child abuse images compared to those available in the 1970s and 1980s "depict sexual violence with a far more sinister tone."[3] The abuse of digital innovation such as the Internet[4] and other technologies[5] has, of course, exacerbated the problem, and continues to do so in a myriad ways. The view of the National Child Exploitation Coordination Centre[6] is that:

> The Internet has changed the way child sexual exploitation offences are committed, investigated and prosecuted. It has also destabilized the ability of Canada's criminal justice system to respond effectively to this type of criminal activity.[7]

The technology has allowed greater access to online child abuse images and has allowed child pornography "communities" to network. For example, in the recent successful investigation and prosecution of Timothy Cox, a British man who ran an online chat-room called "Kids the Light of Our Lives", investigators found 75,960 indecent images of children on Cox's computer, and evidence that he had supplied 11,491 images to other site users.[8]

---

[2] Chief of the Child Exploitation and Obscenity Section, United States Department of Justice

[3] In his presentation, Andrew Oosterbaan stated that in the decades of the 1970s and the 1980s, typical images involved naked children standing, sitting or lying down (*U.S. v Dost*, 636 F. Supp. 828 (S.D. Cal. 1986); see *U.S. v Ferber*, 588 U.S. 747, 752 (1982); *U.S. v Petrov*, 74 F. 2d 824 (2d Cir. 1984)). However, over the past decade, examples now include a father penetrating his 11-month old son's rectum and mouth (*U.S. v Wright*, 373 F.3d 935, 938 (9th Cir. 2004)); young naked girls bound and chained with two and a half inch metal collars and dog leashes (*U.S. v Parmelee*, 319 F.3d 583 n.3 (3d Cir. 2003)); and penises, bottles pacifiers and bananas inserted into the vaginas of young girls and babies (*U.S. v Parmelee*, 319 F.3d 583 n.3 (3d Cir. 2003) at 585).

[4] Such as greater bandwidth and transmission speeds.

[5] Such as the greater availability of webcams and streaming technologies.

[6] The National Child Exploitation Coordination Centre (NCECC), a part of Canada's National Police Services, which is the national clearinghouse and coordination centre created to help protect children from online sexual exploitation. For further information about the NCECC and the work in which it is involved, see the NCECC website at http://ncecc.ca

[7] Found on the NCECC website at http://ncecc.ca/index_e.htm accessed on July 15, 2007

[8] D'Arcy Doran, "Global pedophile ring busted; 31 children rescued" *Seattle Times* June 19, 2007 accessible from here: http://seattletimes.nwsource.com/html/nationworld/2003753353_pedo19.html (accessed on October 25, 2007)

The effect of the Internet has also had wider implications with respect to its impact on children in general. Namely, Oosterbaan notes that the networking of child pornography communities has had the following consequences:

1. It has normalised the idea of child exploitation within the communities;
2. The children involved (and perhaps all children) are dehumanised; and
3. Those involved in these activities are desensitised, which leads to an escalation of the nature of the offence.[9] Oosterbaan observed that the progress of technology has clearly advanced the offence. For example, the development of video streaming has allowed the actual offence to be documented and watched, and child exploitation can take place live online.[10]

In addition to the child pornography offences, the technology has facilitated new dimensions of existing problems such as cyber-bullying and other youth-on-youth exploitation. It has also had serious implications for privacy.

As with the First Symposium, in the Second Symposium these issues were discussed and several themes recurred. Some of these themes reflected ongoing concerns, and others highlighted more novel problems, together with advancing insights. These themes informed and prompted the recommendations made in Part 1 and explained in greater detail in Part 3, and revolved around the issues of:

- education strategies;
- the adequacy of current child pornography legislation;
- privacy, identity, youth and law; and
- the new ways in which child exploitation can take place, particularly via self-exploitation or in a peer on peer context such as cyber-bullying.

[9] Andrew Oosterbaan presentation made at the Second Symposium, available from here: http://www.innovationlaw.org/AssetFactory.aspx?did=243 (accessed on October 25, 2007)
[10] Oosterbaan presentation, note 9.

One further underlying theme which should inform our thinking about strategies and responses to online child exploitation is the understanding of the evolving nature of the child. There appears to be growing recognition of the fact that the term "children" can refer to youth in varied stages of development and this is reflected in the understanding of the evolving nature of children. In this paper we use the term "children" to refer to children generally under the age of 13, and "youth" or "adolescents" to refer to older teenagers.

An important indication of the gains achieved is that those involved in the effort to combat this problem are, as a group, much better informed on many levels. While the problem itself has not necessarily changed, our understanding of it has matured.[11] One example is the issue alluded to above: as we come to understand the nature and extent of the issue of online child exploitation, the analysis is being informed by an increasingly nuanced understanding of the nature of childhood,[12] what the construct of "childhood" means with respect to the law,[13] and how the image we hold of children is impacted upon by the representation of children by and in the media.[14]

Further, there is recognition that this problem is broader than merely the production, distribution and collection of child pornography images, or the archetypal image of the online stranger luring children on the Internet for their own exploitative purposes. The offences relating to child pornography were historically based in obscenity provisions; however, the issue (and our understanding of it) now encompasses more than child pornography. The issues include, but are not limited to examples of youth exploiting other youth, the complicit youth in an exploitative relationship with an adult, online grooming and the phenomenon of cyber-bullying. We should thus examine and refine current policy approaches, in order to ensure that it is capable of encompassing all, or as many as possible, of the potential implications arising under the banner of online child

[11] Oosterbaan presentation, note 9.
[12] Christine Piper presentation made at the Second Symposium, available from here: http://www.innovationlaw.org/AssetFactory.aspx?did=244 (accessed on October 25, 2007)
[13] Carol Rogerson presentation made at the Second Symposium. No presentation slides are available.
[14] Patricia Holland presentation made at the Second Symposium, available from here: http://ww.innovationlaw.org/AssetFactory.aspx?did=242 (accessed on October 25, 2007)

exploitation. It also asks serious questions in respect of how we deal with privacy and the effect of the nexus of law, technology and youth.[15] Also, a great deal of important work has been done that has resulted in a much richer understanding of victim[16] and offender profiles.[17] This in turn will allow the development of risk assessment tools as well as further education and awareness tools.

The next section of this paper revisits first recommendations made following the First Symposium, followed by a more detailed discussion of our current recommendations.

2.1 First Symposium recommendations

It is not the purpose of this report to measure and provide an analysis of exactly what gains have been made in combatting online child exploitation. That is the job of a further study, the importance of which should not be underestimated, and should be undertaken by a third party such as a research institution or a non-governmental organisation. Rather, in this white paper we wish to revisit the recommendations made after the First Symposium on online child exploitation (the "2005 Recommendations") in order to further our understanding of this problem and to provide further tools to aid the effort to counteract it. To this end, David Butt[18] noted that the problem of child exploitation is multi-faceted, and as such it is critical that we have effective communication between the various institutions involved in the effort to stem the problem. Links between institutions, agendas and expertise should be encouraged and supported, as no one person or organisation can effect sustainable change alone. The multi-faceted nature of online child exploitation is succinctly described by Oosterbaan: "A lot of people have to be influenced for you to make progress."[19]

---

[15] Andrea Slane presentation made at the Second Symposium, available from here: http://ww.innovationlaw.org/AssetFactory.aspx?did=248 (accessed on October 25, 2007)

[16] Janis Wolak Presentation made at the Second Symposium, available from here: http://ww.innovationlaw.org/AssetFactory.aspx?did=249 (accessed on October 25, 2007)

[17] Michael Seto presentation made at the Second Symposium, available from here: http://ww.innovationlaw.org/AssetFactory.aspx?did=247 (accessed on October 25, 2007)

[18] David Butt presentation made at the Second Symposium, available from here: http://ww.innovationlaw.org/AssetFactory.aspx?did=240 (accessed on October 25, 2007)

[19] Oosterbaan presentation, note 9.

The 2005 Recommendations are appended at Appendix C and while we will not examine these in detail, it is worthwhile to briefly recall them here. The 2005 Recommendations presented four approaches: international cooperation in investigations, advanced training for police forces and prosecutors, corporate citizenship of Internet Service Providers (ISPs) and educational programs for young Internet users.

In the section dealing with international harmonization, the 2005 Recommendations urged immediate attention to consolidating databases containing hash values of known child exploitation images; updating mutual legal assistance treaties; forging legal instruments necessary to allow functional investigative information sharing internationally; establishing sentencing guidelines which directed judicial attention to the seriousness of the nature of child pornography offences. A further recommendation made in this section was that the term "exploitative" in respect of the prohibited element of sexual relationships involving youth between the ages of 14 to 17 years be clarified. It was also recommended that an online grooming offence be added to the Criminal Code, and this recommendation has been implemented.

The section regarding resources and training for police and prosecutorial services contained recommendations that suggested further resources for police training. Particularly, it was recommended that police should be educated about the element of youth complicity in online meeting crimes, and also that police efforts with respect to child abuse should be coordinated with efforts in child pornography situations. Support programs to deal with the complex emotional issues encountered by victims of online meeting crimes were recommended, as well as counselling programs aimed at young offenders who may themselves have been the victims of abuse. In this section, the 2005 Recommendations advocated that special prosecutors with experience in prosecuting these crimes handle child exploitation cases, and that policing efforts should continue to collaborate with ISPs and government. Further, collaboration should be initiated with hardware and software developers. One example of successful involvement by software developers in the law enforcement effort is the Child Exploitation Tracking System,

jointly developed by Microsoft, the Royal Canadian Mounted Police and the Toronto Police Service.[20]

In the section regarding the role of ISPs and related industries, the effective self-regulation of the ISPs was recommended, by facilitating communication between ISPs that are not members of industry associations and sources of legal information and best practices. Further, a trust certificate program that would encourage the implementation of child protection features by ISP members was recommended. In the 2005 Recommendations the unique position of ISPs as "gatekeepers" was also stressed and the potential for information dissemination and education afforded by this position. ISPs were encouraged to take an active role in educating subscribers about online child exploitation: most large ISPs have taken up this call. This could include publicising information about cybertip.ca (the Canadian national tipline); providing government sponsored resources that clarified what child pornography is, and also guidance about what to do if one happens upon child pornography online. It was recommended also that ISPs should be made aware of their legal obligations and of the voluntary efforts they can engage in to assist law enforcement. There continues to be some confusion about whether ISPs may disclose basic subscriber information to law enforcement upon request, or whether such disclosure would be contrary to federal privacy legislation.[21] We would urge clarification of this issue, as it has been a key achievement of voluntary ISP cooperation with police.

In addition to existing legal obligations, the 2005 Recommendations noted that ISPs should be required to disable access to child pornography materials upon notice from a designated law enforcement entity and should be required to report child pornography materials encountered on their facilities. It further recommended that incentives for the development of technical tools be established.

[20] For more information, see http://www.microsoft.com/presspass/features/2005/apr05/04-07CETS.mspx (accessed October 12, 2007).
[21] See *Re: S.C.* 2006 ONCJ 343.

Finally recommendations were made in respect of education, which addressed specific populations. Namely, it was recognised at the time that the educational needs of children under the age of 12 would generally differ from those of older youth, especially as there can be an element of youth complicity with respect to victims who are older youth. Further education and awareness-raising campaigns for parents and the public with respect to the "real" nature of online child exploitation offences was also recommended.

The recommendations made in this report build on the 2005 Recommendations and focus particularly on themes that recurred in the Second Symposium. The result of this effort is new recommendations focusing on education, cyber-bullying and legal reform. This should not be read to mean that the recommendations made with respect to the other approaches no longer require attention. Rather, we focus on these particular areas to highlight the fact that further immediate action should be taken in the areas singled out in this report. Where the 2005 Recommendations have not been addressed, we urge that they be revisited.

We reiterate the sentiment expressed in the 2005 Recommendations, namely that:

> All solutions suggested in this paper should be implemented in consultation with the Privacy Commissioner, and with a view to protecting fundamental rights with 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.[22]

Further, as a general matter, we recommend that the collaboration that has already occurred between various institutions and stakeholders (such as ISP industry and law enforcement) be further encouraged and sustained.[23]

[22] White paper following the First Symposium at p 11.

[23] One instance of this was provided by David Butt in his presentation at the Second Symposium, and this is the effort of the National Child Exploitation Coordination Centre, an integral part of Canada's National Police Services, which is reconceptualising the role of policing and education. For more information, see http://ncecc.ca/index_e.htm (accessed October 12, 2007)

3 2007 Recommendations in detail

3.1 Education

1. Target educational campaigns to at-risk youth and articulate the reality of online grooming and youth-on-youth exploitation

Education and awareness responses should speak directly to children and youth, and it is important that these responses resonate with the targeted youth audience, particularly at-risk youth. The apparent consensus from the Second Symposium is that good educational resources are now available, but strategies to position the educational material to specifically target at-risk youth should be developed. The concern is that the material is received by already-wary youth, but that at-risk youth are still not reached. This is likely to prove to be the key challenge as youth may not recognise the adverse effects of certain behaviour on themselves, such as making sexual images of themselves available online, even to one person. We should also interrogate why it is that while there is greater awareness and understanding of the problem, some youth still engage in risky behaviour.

The work presented by Janis Wolak on behalf of the Crimes against Children Research Centre (CCRC)[24] and by Ethel Quayle[25] is invaluable for gaining insight into the profiles of victims, particularly in luring offences. This work provides us with a sophisticated understanding of victims, the effect of the Internet and, the factors that make youth vulnerable to exploitation not only to child pornography in the "traditional" sense, but also self-victimisation, the exploitation of youth by other youth, and online grooming.

The CCRC carried out large scale surveys of Internet users aged between 10-17 years. The first interview was undertaken in 2000, and the second in 2005, and the survey respondents were asked about unwanted sexual solicitations in the past year. The findings of this survey were interesting: between 2000 and 2005, fewer youth reported unwanted sexual solicitations. The CCRC also found that this decrease can be attributed to the fact that fewer youth were talking online to unknown people, forming close online

[24] Funded by the National Center for Missing & Exploited Children and US Department of Justice, OJJDP
[25] See Ethel Quayle presentation made at the Second Symposium, available from here: http://ww.innovationlaw.org/AssetFactory.aspx?did=245 (accessed on October 25, 2007).

relationships with unknown people and going to chatrooms. Wolak suggested also that five years of prevention education may have contributed to this trend.

However, there has been no decline in aggressive solicitations, where solicitors have made or tried to make offline contact. Wolak notes that these are the solicitations most likely to evolve into crimes. Further, in the second survey, a new concern has arisen as 4% of youth Internet users said that in the past year, solicitors asked them to take sexual photographs of themselves and to send the photographs online to the solicitors. Apart from the obvious dangers, this raises serious privacy issues that may not have effective recourse, legal or otherwise. Further, there has been an increase in unwanted exposure to sexual material and online harassment, despite increased use of filtering, blocking and monitoring software.[26]

In respect of online grooming, the CCRC's work provides interesting findings. The victims are usually young adolescents. The perpetrators find, befriend and romance victims and bring up the topic of sex. Deceit is rare regarding the perpetrators' true age or sexual intentions. Violence, abduction and stalking are also rare. Many victims feel love or close friendship for the perpetrators, as most seduce their victims. Quayle notes also that a surprisingly large and often ignored number of the perpetrators of these offences are other young people (citing Finkelhor et al., 2001; 2006).

With respect to factors that increase vulnerability in youth, CCRC's work has highlighted that it is not naiveté or inexperience that make youth vulnerable. Just as young Internet users are becoming more Internet savvy, older teenagers between the ages of 14 and 17 years who are sophisticated Internet users continue to engage in more complex and riskier Internet use. However, posting personal information online and keeping online journals or blogs are online behaviours that are not directly related to receiving aggressive solicitations. Factors of vulnerability include:

- the normal adolescent interest in sex;
- being a girl;

[26] Ethel Quayle presentation, citing Finkelhor, Wolak et al., 2006, note 24.

- being a gay or questioning boy;
- having a history of sexual or physical abuse; and/or
- interacting online indiscriminately with unknown people. Wolak states that this is not typical youth behaviour, but rather stems from the desire and psychological need to form relationships.

Youth who engage in a pattern of a variety of different types of risky online behaviour are also more vulnerable, where the greater the variety of risky behaviours engaged in, the higher the risk. Potentially risky behaviours include aggressive and sexual behaviour, interacting online with unknown people and the disclosure of personal information.[27]

It is also important to bear in mind Wolak's point that adolescent sexual development and Internet exploration generally go hand-in-hand, and that sexual exploration is healthy. Wolak also states that it is important to describe the problem of online grooming accurately, and avoid descriptions of the problem that characterise the victims as young children, or that over-emphasize violence or deception. Wolak argues that the approach taken should be that of risk-reduction. For example, instead of disallowing the posting of personal information at all, we should inform and empower youth with respect to being aware of privacy settings. Further we should be frank with youth about online sexual activities such as going to x-rated chatrooms, talking about sex with people they meet online, looking at pornography and cybersex. One useful strategy would be to provide examples and warning signals of online interaction (whether adult-on-youth or youth-on-youth) that is or tends towards being abusive so that victims or potential victims who are currently engaging in risky behaviour have concrete indicators by which to identify risky situations.

The recognition that sexual exploration by youth is healthy must also be balanced with the insight provided by Quayle's work in respect of the online activities of youth. She

[27] CCRC's work identified nine potentially risky behaviours: (1) posting personal information – 56%; (2) interacting online with unknown people – 43%; (3) having unknown people on a buddy list – 35%; (4) making rude or mean comments – 28%; (5) sending personal information to unknown people – 26%; (6) using file sharing to download images – 15%; (7) going to x-rated web sites on purpose – 13%; (8) harassing people youth are mad at – 9%; and (9) talking to unknown people about sex – 5%.

highlights the findings of the Barnardos survey (Palmer, 2003) which show that youth also place sexual images of other youth online, youth view adult pornography, and both adults and youth have cybersex with youth.[28] Quayle points out also the findings of various studies which illustrate that while youth are viewing violent and/or highly sexualised websites accidentally, this viewing is also in some cases intentional. For example, in the survey of 1500 youth carried out by Wolak et al., in 2005, 42% of the youth survey reported exposure to online pornography. Of these, 34% was wanted exposure. In respect of these findings, Quayle stated:

> A notable finding was the perception of exposure to sexually explicit websites on oneself… participants perceived no impact on themselves… [This] may be problematic because previous research had documented negative effects of exposure to sexually explicit content… It may be that adolescents are developmentally unable to judge how this content affects them…While it might not be possible to precisely define what constitutes normal sexual behavior, there should be concern for young people with a relatively narrow perspective who are exposed to frequent images of behaviors such as sodomy, group sex, sadomasochistic practices, and bestiality" (p 120) (Kanuga and Rosenfeld (2004)[29]

She further cites the study undertaken by the New Zealand Censorship Compliance Unit which finds that one of the largest single groups of offenders with respect to illegal images were aged between 15-19 years, where the activities included downloading, trading and producing abuse images.[30] This group is also more likely to trade and/or possess images of teenagers and/or older youth than any other group of individuals, and the most likely to select material showing children and youth with others of their age. However, all possessed images of children and young people engaged in explicit sexual activity, including images of children aged between 2 and 7 years.

Thus, the education response must acknowledge and identify youth-on-youth interaction that can be healthy, but make clear that youth-on-youth interaction can also be abusive or

---

[28] Ethel Quayle presentation, note 24.
[29] Ibid.
[30] Ibid. A copy of the 2004 profiling research is available from here: http://www.dia.govt.nz/pubforms.nsf/URL/profilingupdate.pdf/$file/profilingupdate.pdf (accessed November 20, 2007)
For a 2007 summary update of the profiling research see: http://www.dia.govt.nz/Pubforms.nsf/URL/Profilingupdate3.pdf/$file/Profilingupdate3.pdf (accessed November 20, 2007).

exploitative. This brings us to the crucial issue of teaching youth how to manage and protect their own sexual identity and integrity.

2. Educate youth to understand the concept of sexual identity and equip youth with strategies to manage and protect it

The issue of sexual identity is pertinent when we consider that Quayle's work has unearthed the trend where youth create and make available highly sexualised images of themselves, or allow these images to be made by others and posted online. Camera phones, webcams, chatrooms, blogs, instant messaging and social networking networks enable young people to share sexual images of themselves or of others, and these images may expose the youth to sexual solicitation by adults or to extortion for further sexual images (typically, via threats that the sexual images will be revealed to parents if further sexual images are not supplied). Thus while keeping and reading blogs, posting personal information online and using online social networking applications may not be activities which in themselves increase the risk of aggressive solicitation, a study by Longo (2004) cited by Quayle concludes that these behaviours remain of concern because they can expose children and youth to incorrect information about human sexual behaviour; provide exposure to age inappropriate sexual materials; have the potential to develop sexually compulsive behaviour in youth and to develop sexual 'addiction'; and enhance deviant sexual fantasies. That is, inappropriate content can be posted on blogs and online journals that are either maintained by youth, or on those that youth are reading. A quick search on, for example, a blog search engine such as www.technorati.com for tags such as "porn" yields numerous pages of age-inappropriate search results.

In addressing this issue (and the broader issue), it is again important to acknowledge that adolescent sexual development and Internet exploration typically go hand in hand, and that healthy sexual exploration via the Internet needs to be acknowledged when talking to youth. In doing so, it is important to realise that there is a growing recognition of the "evolving" nature of childhood. Carol Rogerson[31] points to the United Nations Convention on the Rights of the Child (UNCRC) for evidence to support the notion of the

[31] Carol Rogerson presentation, note 13.

"evolving" nature of the child, rather than the binary of "child" and "adult". She highlights Article 5 as an example, which provides that States accept parental authority with respect to the evolving capacity of the child. That is, parents have to respect the fact that children will have an evolving capacity as they move through developmental stages, and "under 18" does not necessarily represent a homogenous group of people.

This therefore increases the importance of education campaigns to raise youth awareness in respect of the idea of one's sexual identity and its integrity and to equip youth with strategies to manage and protect this. There are already comprehensive resources available with respect to teenage sexuality,[32] but media literacy should be emphasised. What is available in a variety of media can expose youth to a high level of sexual imagery, implicit (and sometimes explicit) in which there are many messages about sexuality which may not always be healthy or appropriate for youth. One example of a media literacy campaign has been developed by Vancouver Coastal Health which attempts to promote a critical approach for youth towards media, to create awareness of how media affect/create perceptions of reality, particularly in respect of what it means to be male or female, and to explore ways of limiting the harms that can be caused by media.[33] This campaign does not address exposure to explicit sexual images, however.

These campaigns could be integrated into sexual health education at schools, and should include discussion of how the Internet and digital technology impacts on the sexual privacy of youth. Media literacy should include a component addressing how youth use media in respect of the content they view, produce and disseminate. It should also highlight the risks associated with allowing digital images of themselves to be taken. It should emphasise to youth that once these images are taken, they will potentially lose control over how these images are used and disseminated. The link between this and the loss of control over their own identities should be emphasised, together with the implications of this loss of control over one's identity. This media literacy campaign should also specifically address the potential harms that can arise from viewing sexually

[32] See for example this summary of the available resources for teenagers: http://www.vch.ca/teensexualhealth/resources.htm (accessed September 2, 2007)
[33] See http://www.vch.ca/teensexualhealth/workshop_modules/media_literacy.htm (accessed September 2, 2007)

explicit and age-inappropriate content online. Industry Canada's cyberwise.ca project goes some distance in addressing these issues, particularly in the section aimed at "Teens", and this content should be updated.[34] However, the critical issue is again ensuring that this material is positioned so that at-risk youth will access it and internalise the message. Evidence shows an increase in knowledge regarding online risks, but little to no change in behaviour (Chibnall, Wallace, Leicht, & Lunghofer, 2006; Crombie & Trinneer, 2003).[35] Some of this lack of effectiveness may well come from a dearth of realistic materials addressing the ways youth use the Internet for sexual exploration, materials and resources which would help youth navigate this difficult aspect of their healthy development.

3.2 Cyber-bullying and Sexual Exploitation

Cyber-bullying differs from traditional bullying as it is indirect; can happen both on and off school property; the victim likely does not know the identity of the bully; it occurs in a way that is typically "under the radar" of adults; and the nature of the fear is different, in that it pervades all areas of the victim's life. We note that cyber-bullying can include sexual exploitation, and urge awareness of these features of the problem. For example, friends who know secrets about friends or former friends can leverage this knowledge for sexual content, and especially girls have been pressured to send nude or sexual pictures of themselves through this type of peer extortion. Further, victims cannot stop private images and communication from being publicly distributed. Youth are coercing other youth online, and the following recommendations aim to address this new aspect of online child exploitation.

[34] See http://strategis.ic.gc.ca/epic/site/cyby-cybj.nsf/en/h_uz00095e.html (accessed August 28, 2007)
[35] As cited Faye Mishna, in her presentation entitled ""Keeping Our Children Safe: Protecting Them from Cyber Abuse" presented at the conference themed "Securing the Future of our Children," October 26, 2006; organized by the RBC Chair in Public and Economic Policy and the RBC Chair in Applied Social Work Research in association with the School of Public Policy and Governance at the University of Toronto.

1. Engage in further research and multidisciplinary collaboration to enable, among other progress, legislative clarification and development.

Faye Mishna, McCain Chair in Child and Family, Faculty of Social Work, University of Toronto and participant in the 2005 white paper recommendations, is part of a study which is currently undertaking a systematic review of the problem of cyber-bullying with the Campbell Collaboration.[36] The project aims to examine prevention and intervention programs in order to synthesize available knowledge and to inform further research and policy.[37] This program includes a partnership with the Toronto District Schools Board and the UJA Board of Jewish Education to conduct a survey of middle, junior and high school students to determine the prevalence, impact, and response to cyber bullying. This survey will also include parents, teachers and principals. We support funding such projects and suggest that they be expanded to include multidisciplinary collaboration, for instance between Law and Social Work in order to ascertain the nature and extent of cyber-bullying in relation to the approaches and efforts in Canada and internationally to address this issue. The results of such a collaboration would provide empirical evidence of the experiences of victims and a profile of those who engage in cyber-bullying, as well as a collation of best practices across jurisdictions. This study could be, for example, aligned with existing provincial government strategies, such as the Ontario Ministry of Education's current Safe Schools strategy.[38] It is critical that in the course of these studies the definition of bullying include an awareness of the ways that peers use sexuality to bully other peers.

We note that the work of the CCRC in New Hampshire was initially funded by the US Department of Justice, Office of Juvenile Justice and Delinquency Prevention.[39] A

[36] The Campbell Collaboration is an international network of social scientists who produce, maintain and disseminate systematic reviews of research evidence on the effectiveness of social interventions, particularly in respect of education, crime and justice, and social welfare. More information is available from here: http://campbellcollaboration.org/About.asp (accessed November 18, 2007)
[37] Faye Mishna presentation slides.
[38] Safe Schools Action Team, *Shaping Safer Schools: A bullying prevention action plan* (Ontario, 2005) online at http://www.edu.gov.on.ca/eng/healthysafeschools/actionTeam/shaping.pdf (accessed on August 25, 2007).
[39] See http://www.unh.edu/ccrc/about-ccrc.html#s6 (accessed on August 25, 2007).

similar model might be pursued in Canada, as this would also bring together various disciplines for a more coordinated approach to this issue.

2. Provide parents, teachers and other guardians with immediate "hands-on" responses to cyber-bullying.

If we consider cyber-bullying through the lens of privacy of the victims, we should ask how we can create safe spaces. Mishna suggests a multi-pronged strategy, parts of which can already be implemented as a way forward. A technological response can be implemented by blocking access to unapproved sites and filtering graphic descriptions and images. However, it is important to note that while this response is able to reduce exposure to inappropriate content, it will not eliminate it (Schneider, 1997; Hunter, 2000; Mitchell, Finkelhor, & Wolak, 2003). Further, such measures might block benign content, and youth will find ways of circumventing this technology. To supplement the technological response, Mishna notes that parental supervision is significant and that household rules do make a difference. With no rule about "sites not to visit" 43% in grades 6 and 7 visited offensive sites and 49% in grades 10 and 11 visited offensive sites. This is contrasted where there are rules about "sites not to visit", 14% in grades 6 and 7 visited offensive sites and 33% in grades 10 and 11 visited offensive sites (Young Canadians in a Wired World, 2005)[40]. In addition to rules about sites and inappropriate content, Mishna notes that 74% of households surveyed now also have rules about meeting online acquaintances offline (Young Canadians in a Wired World, 2005). Essentially, Mishna's view corresponds with that of Wolak's, and she argues that it is ineffective to deny youth Internet access as a means to protect or punish. She argues instead that the responses must be creative to protect and encourage youth to communicate with parents and/or other adults. These messages must also be communicated effectively to parents and other guardians whether at home or in some other protected context.

[40] Available from here: http://www.media-awareness.ca/english/research/YCWW/index.cfm (accessed on August 25, 2007)

Further, other campaigns around poor decision-making that have enjoyed some level of success such as anti-smoking and drunk-driving campaigns can provide insight into shaping a public information and awareness response. This is necessary, even if only to raise public awareness about the existence and seriousness of cyber-bullying. It is further necessary in order to alert children who are targets of cyber-bullying to the fact that they should not suffer this abuse quietly and alone; rather, there are people in a position to help who are willing to do so.

3.3 Legal recommendations

1. Balance the approach taken by the current child pornography provisions in the Criminal Code by uncoupling the "broad net" approach to offences from punitive mandatory sentencing regime.

Canada's online child exploitation provisions were examined again in the Second Symposium, and were questioned in one significant way. Bruce Ryder argues that section 163.1 of Canada's Criminal Code has both a "solid and urgent moral core and a morally dubious periphery"[41] and that current mandatory sentencing provisions apply to offences at the core. The solid moral core is supported by a powerful rationale: to deter the abuse of children by punishing all elements of the supply and demand. Ryder notes that Criminal Code section 163.1 has proven to be a powerful weapon against those who use the Internet to distribute and use child abuse images, as witnessed by a dramatic increase in prosecutions since the late 1990s, where the majority of these prosecutions involved possession charges regarding the images of the abuse of pre-pubescent children. Ryder further notes that guilty pleas are the norm and acquittals are rare.

In the 2005 round of amendments, mandatory minimum jail sentences for all those convicted of child pornography offences committed after November 1, 2005 were introduced This minimum mandatory sentence is one year for the making or distribution of child pornography, and 45 days for possession or accessing these images. Ryder notes that there is support for a more punitive approach from the judicial system as well, with

[41] Bruce Ryder presentation, available from http://www.innovationlaw.org/AssetFactory.aspx?did=246 (accessed on August 20, 2007)

sentencing practices becoming progressively more severe, and conditional sentences increasingly rare.

However, Ryder argues that it is the periphery of the child pornography offence that is contentious. This argument is consistent with the majority view of the Supreme Court of Canada in *R v Sharpe*[42]. The SCC by and large upheld the law, but split on "peripheral" aspects. The majority held that the law went too far in some instances, and the interests of child protection will not justify all of the law. One example of the law going too far was to criminalise the possession of pictures by teenagers of themselves, and of lawful sexual activities between themselves and their partners for personal use.[43] The majority thus carved out from criminalisation these images. McLachlin CJ held that:

> Such materials could conceivably reinforce healthy sexual relationships and self-actualization. For example, two adolescents might arguably deepen a loving and respectful relationship through erotic pictures of themselves engaged in sexual activity. The cost of including such materials to the right of free expression outweighs any tenuous benefit it might confer in preventing harm to children.[44]

Ryder takes up this argument and states that at the periphery, the child pornography provisions are liable to cause more harm than it prevents. Ryder states that, in addition to the material carved out of the legislation by *Sharpe*, the moral periphery of the offence also embraces materials that are not records of child abuse and subjects them to the same stigmatizing and punitive regime. These include images such as those depicting adolescents or young adults in sexual poses or engaged in lawful sexual activity; and creative works that are products of the imagination, including stories and paintings. Such a stance does not reflect the evolving nature of childhood and may indeed be inconsistent with the healthy sexual development of youth. Instead, a more nuanced series of offences is required. If, for example, mandatory sentencing is to remain part of the legislation, it

[42] *R. v. Sharpe*, [2001] 1 S.C.R. 45
[43] 14 years is the age of consent, so sexual activity between 14-17 year olds is considered lawful.
[44] *R. v. Sharpe*, note 50 at [109]. The majority in *Sharpe* appears to have placed priority on concepts of teenage agency and autonomy, which requires that teenagers, as rights-holders, should enjoy privacy and freedom of expression. However, the opinion of L'Heureux-Dubé J is interesting as she took a more protectionist stance and disagreed with McLachlin CJ and held that these images are harmful self-indulgences and are not useful for self-actualisation. She found that these images were harmful to teenagers themselves and could be used to perpetuate unhealthy attitudes and could be used to harm other children (*R v Sharpe*, note 50, particularly at [183] – [186])

should be targeted only at the worst types of offences. It might therefore be useful to have a separate regime that deals with "youth exploitation images." This would achieve an uncoupling of the worst types of offences that deserve a more punitive sentencing regime, but avoid the harms of a broad net approach.

Further, we must be clear about the purpose of these laws. If the legislative regime's purpose is to protect children, then it would be useful and important to be explicit in defining child pornography as "child abuse images" or "child sexual abuse images" so that it is clear the harms that the legislation is intending to target. On the other hand, if the law intends to stay true to its obscenity origins, then more consistency should be attempted between the child pornography provisions and other obscenity provisions. In addition to the protection of individual children, there is the argument that images of child abuse should be subject to legal sanction because, analogous to hate speech, they undermine the value we place in children as a culture and so do harm to the category of children as a whole. The tension between protecting the collective humanity of children and risking legislative overreach is a delicate one but arguably can be best addressed not by limiting the scope of these provisions but by ensuring that the sentencing regime is appropriate to the different kinds of images in circulation.

2. Reconsider focus on fixation and recording to address the existence of streaming technology.

The Criminal Code provisions for child pornography and luring have technological components. That is, a visual or aural recording of sexual activity by young people is deemed by the law to be of a different character than engaging in sexual activity itself, as illustrated by the fact that public dissemination of visual, written or audio representations of lawful sexual activity between young people falls within the child pornography prohibitions.[45]

[45] *R v Sharpe* note 50 at [99], which exempts youth-made recordings "exclusively for personal use" from the child pornography provisions.

Recording is only one technologically-enabled problem, however, and the popularization of streaming technologies has introduced a new facet to online child exploitation, regardless of whether fixed images are made. The case of Timothy Cox, mentioned above, emphasises the urgency of this harm. In that case, Cox ran a chatroom that also streamed live videos of children being sexually abused in addition to being a forum for the exchange of photographs and videos. The accessing offence should certainly capture the wrongs committed by live online audiences in such cases, even if the images are never fixed, but it would be helpful to clarify that the broadcast of live performances falls within the definition of "visual representation" in the Criminal Code, even where no fixed recordings are made. This clarification would also help to articulate for older young people the dangers that arise from interacting via webcam, where what may appear to be a live exchange with a boyfriend or girlfriend could potentially be shared more publicly.

3. Legislate to allow victims of child pornography civil redress against offenders.

Technology can now be used in increasingly intrusive ways, impacting on an individual's ability to control his or her own identity, and this is particularly true for victims of online child exploitation. The rapid pace of development and innovation of digital technologies has resulted in the situation where these technologies can be used to seriously affect an individual's privacy, potentially without legal consequence. Inevitably, the technology will continue to evolve, and the potential for the abuse of these technologies by individuals will keep pace. The criminal law recognises that the harms accruing to victims as a result of child pornography can be further augmented by the widespread dissemination that can be achieved online. However, the criminal law in Canada does not currently provide an avenue for providing civil redress for the loss of dignity and control of the victim's identity that results from child pornography activities. We therefore suggest that a cause of action be created, or the availability of an existing cause of action be clarified, in order to allow victims of child pornography to sue those convicted of disseminating or possessing images of their abuse for invasion of privacy.[46]

[46] Four common law provinces have enacted statutory privacy torts: 1) British Columbia -- Privacy Act, [RSBC 1996] Chapter 373 available online from here: http://www.qp.gov.bc.ca/statreg/stat/P/96373_01.htm. Under this Act, an invasion of privacy is where a person 'wilfully and without a claim of right' violates the privacy of another. No proof of damage is

The privacy interest of victims of child pornography is well-recognised in the case law. Further, the exploitative image of a child impacts on his or her privacy interests in a continuing way as the image can be continuously disseminated. The majority decision in *Sharpe* expressed this concern and emphasised the ongoing trauma these images of child abuse represent, thus reinforcing the necessity for recognition of the victim's privacy rights in this context:

> The child is traumatized by being used as a sexual object in the course of making the pornography. The child may be sexually abused and degraded. The trauma and violation of dignity may stay with the child as long as he or she lives. Not infrequently, it initiates a downward spiral into the sex trade. Even when it does not, the child must live in the years that follow with the knowledge that the degrading photo or film may still exist, and may at any moment be watched and enjoyed by someone.[47]

This ongoing harm of knowing that these degrading images exist and are being disseminated is potentially addressed by a privacy tort, where people who disseminate or collect child abuse images can be sued by the victims who appear in those images.

Further, in respect of consenting actors (rather than victims of abuse), consenting to the taking of an image (which under *Sharpe* may be legal) does not equate to consent to the dissemination of the image (which remains illegal). Harm is therefore also done in the privacy violation occasioned by dissemination, whether or not the image itself was degrading at the time it was taken. Cases are emerging all over the world where ex-boyfriends and girlfriends disseminate sexual images of once-consenting partners after a teen romance goes sour. This sort of peer exploitation may be best addressed via an invasion of privacy tort. While we do not want to advocate for an explosion of teen to

---

required for the tort to be actionable; 2) Saskatchewan -- Privacy Act , R.S.S. 1978, c. P-24 available online from here: http://www.canlii.org/sk/laws/sta/p-24/20060412/whole.html. The tort is set out very broadly in section 2: It is a tort, actionable without proof of damage, for a person wilfully and without claim of right, to violate the privacy of another person; 3) Manitoba -- Privacy Act, C.C.S.M. c. P125 available online from here: http://www.canlii.org/mb/laws/sta/p-125/20060412/whole.html; and 4) Newfoundland -- Privacy Act, R.S.N.L. 1990, c. P-22 available online from here: http://www.canlii.org/nl/laws/sta/p-22/20051121/whole.html. In Quebec, Article 5 of the *Charter of Human Rights and Freedoms* provides that "every person has a right to respect for his private life." These torts are general in nature and are not aimed towards the issue of online child exploitation, but could reasonably be applied to a child pornography scenario.

[47] *R v Sharpe* note 50 at [92]

teen lawsuits, an invasion of privacy tort that clearly applies to these situations could at least serve as a normative guide to teen behaviour.

The provinces and/or federal government should enact or clarify the availability of existing causes of action that would allow victims and the families of victims to seek civil redress from offenders. In addition to existing provincial privacy torts[48], an example of the creation of a civil cause of action in the criminal law can be found in the Codified Laws of South Dakota, the relevant provisions of which are attached as Appendix D.[49]

3.4 Risk assessment tools for sentencing

1. *Develop risk assessment tools to be used in sentencing, and use existing research in doing so*

Some of the concerns about the moral periphery of the child pornography offences can also be addressed through appropriate sentencing. We recommend focusing on the development of risk assessment tools that should inform sentencing practices, as risk assessment tools can be invaluable to appropriate and effective sentencing practices.

Michael Seto's team with the University of Toronto and the Centre for Addiction and Mental Health focuses on risks of sexual offending posed by child pornography offenders. Work from a 2006 study indicated that child pornography offending is indicative of paedophilia. However, what is most indicative of risk of offending against children and of recidivism is whether paedophilia combines with anti-sociality. The following table reproduced from Seto's presentation summarises these findings:

[48] See footnote 46 above.
[49] SB 184 "An Act to protect the children of South Dakota against sexual exploitation by criminalizing certain conduct involving children and the internet, to provide for civil remedies, to require certain people to report suspected violations, and to revise certain provisions regarding the unlawful use of computers" amended the South Dakota Criminal Code, Title 22, Chapter 24A. For a discussion on Bill SB 184, see http://www.state.sd.us/homeland/Press/press_2.27.2002.asp (accessed August 25, 2007).

Predictions regarding risk of child pornography offenders

		Paedophilia: No	Paedophilia: Yes
Antisociality	No	Relatively unlikely to reoffend.	Child pornography recidivism.
	Yes	Some risk to offend against children.	High risk to offend against children.

The existence of paedophilia is indicative of the existence of motivation. The level of anti-sociality indicates the extent to which the individual does or does not have the requisite "brakes." A prior study found that a history of violent offence is a good predictor of whether the individual will commit a new sexual offence. Seto's current research is focused on comparing child pornography offenders with a contact sexual offence history to those without a contact sexual offence history. It is also focusing on variables other than criminal history that might be good predictors of risk. These include substance abuse, stability of the individual's lifestyle and other demographics. Further, detailed analysis will be made of child pornography and the content will be coded with respect to age, explicitness and evidence of other paraphilia, such as fetishism. Seto's studies have found that the type of pornography is indicative of sexual preferences, thus the importance of recording the nature of the pornographic content. Further, the new study will focus also on identifying antisocial factors.

This work is significant, especially in respect of the broad reach of the child pornography provisions contained in the Criminal Code. The development of risk assessment tools will allow prioritisation of cases with respect to prosecution and will also allow a more nuanced approach to sentencing. Further, the sentencing of child pornography offenders is also a public health issue, especially when considering the mental health and anti-sociality dimensions of the offence, and this work will allow identification of preferential

offenders (that is, offenders who display paedophilic preferences) and this should impact on treatment issues in sentencing.

3.5 Body parts registry

1. In addition to the national sex offenders' registry, create and implement a searchable database of body parts of sex offenders

As reported in the *National Post*[50] after the Second Symposium, the NCECC conducted a survey of child porn images where it was found that one in four contained at least one identifiable mark on an abuser. However, there is no systematic way for Canadian law enforcement efforts to compare this information with information on known sex offenders. Currently, files from the national sex-offender registry might include descriptive notes, but not pictures of body parts other than the face.

Accordingly, the NCECC has proposed the creation of a searchable database of "body parts" of known sex offenders which might include distinctive features such as tattoos, moles, body hair and scars, as this would be a useful investigative tool. The technology to support such a database already exists. We support the creation of such a database subject to *Charter* scrutiny.

[50] Joseph Brean, "Body-parts registry proposed to fight child porn" *National Post*, May 08, 2007 available at http://www.canada.com/nationalpost/news/story.html?id=d79abff9-6ef3-40cd-a136-1a982922d551&p=1 (accessed October 25, 2007).

4 Conclusion

Online child exploitation continues to be a significant problem, and the evolving nature of technology continues to present new challenges, in the form of novel problems as well as contemporary manifestations of existing problems. Fortunately, much valuable work has been undertaken in the effort to combat online child exploitation. Further, this work is multi-disciplinary in character, and efforts to build links between the various institutions and agendas involved should be nurtured. We reiterate the 2005 Recommendations and where these recommendations have not yet been addressed, we strongly suggest that they be considered as they continue to be relevant. Further, we encourage policy makers and legislators to consider and implement the multi-pronged recommendations made in this report as they represent the materialisation of current and relevant research, and would support the efforts that are already underway, in a manner consistent with the urgent need to combat online exploitation while recognizing that sexual exploration is central to healthy development and growth.

References

Texts

Beran, T. & Li, Q. (2005) Cyber-Harassment: A Study of a New Method for an Old Behavior. *Journal of Educational Computing Research,* 32(3), 265-277

Chibnall S, Wallace M, Leicht C, & Lunghofer L, 2006; *I-Safe Evaluation Report*, US Department of Justice

Crombie, G., & Trinneer, A. (2003). *Children and Internet Safety: An Evaluation of the Missing Program*. A Report to the Research and Evaluation Section of the National Crime Prevention Centre of Justice Canada. Ottawa: University of Ottawa.

Hugh-Jones, S. & Smith, P.K. (1999). Self-reports of short-and long-term effects of bullying on children who stammer. *British Journal of Educational Psychology*, 69, 141-158

Hunter, C.D. (2000). Internet filter effectiveness - testing over- and underinclusive blocking decisions of four popular web filters. *Social Science Computer Review, 18*(2), 214-22.

Kanuga, M., & Rosenfeld, W. D. (2004). Adolescent sexuality and the Internet: The good, the bad, and the URL. *Journal of Pediatric and Adolescent Gynecology* 17, 117-124.

Longo, R.E. (2004). Young people with sexual behaviour problems and the Internet. In M. Calder (Ed), *Child Sexual Abuse and the Internet: Tackling the New Frontier*. Dorset: Russell House Publishing.

Mitchell, K.J., Finkelhor, D., & Wolak, J. (2003a). The exposure of youth to unwanted sexual material on the Internet: A national survey of risk, impact, and prevention. *Youth and Society, 34*(3), 330-358

Mitchell, K. J., Finkelhor, D., & Wolak, J. (2001). Risk factors and impact of online sexual solicitation of youth. *Journal of the American Medical Association, 285(23),* 3011-3014.

Palmer, T. (2003). Just one click. London: Barnardos

Richards, Neil M and Solove, Daniel J, "Privacy's other path: recovering the law of confidentiality" (2007) 96 Georgetown Law Journal (forthcoming)

Safe Schools Action Team, *Shaping Safer Schools: A bullying prevention action plan* (Ontario, 2005)

Schneider, K. (1997). A Practical Guide to Internet Filters. *Neal Schuman Publishing.* Clifton Park, New York

Sullivan C. (2007). Internet Traders of Child Pornography: Profiling research – Update. *Censorship Compliance Unit of the Department of Internal Affairs, New Zealand*

Wilson D, Andrews C. (2004) Internet Traders of Child Pornography and other Censorship Offenders in New Zealand: Updated Statistics (November 2004). *Censorship Compliance Unit of the Department of Internal Affairs, New Zealand*

Wolak, J., Mitchell K.J., & Finkelhor, D. (2006) Online victimization of youth: Five years later. National Center for Missing & Exploited Children. Report #07-06-025 : Alexandria , VA.

Wolak, J., Finkelhor, D., & Mitchell, K.J. (2005). The varieties of child pornography production. In Quayle, E. & Taylor, M. (Eds.), *Viewing child pornography on the Internet: Understanding the offense, managing the offender, helping the victims* (pgs. 31-48). Dorset, UK : Russell House Publishing.

Newpaper articles
Brean J, "Body-parts registry proposed to fight child porn" *National Post*, May 08, 2007
D'Arcy Doran, "Global pedophile ring busted; 31 children rescued" *Seattle Times* June 19, 2007
Hanes A, Brean J, "Online obsessions" *National Post* October 20, 2007

Cases
Autosurvey Inc. v. Prevost [2005] O.J. 4291 (Sup.Ct.)
R. v. Sharpe, [2001] 1 S.C.R. 45
Roth v. Roth (1991) 4 O.R. (3d) 740 (Gen. Div.)
U.S. v Dost, 636 F. Supp. 828 (S.D. Cal. 1986)
U.S. v Ferber, 588 U.S. 747, 752 (1982);
U.S. v Parmelee, 319 F.3d 583 n.3 (3d Cir. 2003)
U.S. v Petrov, 74 F. 2d 824 (2d Cir. 1984)).
U.S. v Wright, 373 F.3d 935, 938 (9th Cir. 2004)

Legislation
Education Amendment Act (Progressive Discipline and School Safety), S.O. 2007 C.14
Education Act, R.S.O. 1990, c. E.2
Privacy Act , R.S.S. 1978, c. P-24
Privacy Act, [RSBC 1996] Chapter 373
Privacy Act, C.C.S.M. c. P125
Privacy Act, R.S.N.L. 1990, c. P-22
South Dakota Title 22, Chapter 24A

Appendix A:

Speaker Biographies

Second International Symposium on Online Child Exploitation

May 7, 2007, University of Toronto

Signy Arnason (Cybertip.ca) is the Director of Cybertip.ca, Canada 's national tipline for protecting children from online sexual exploitation. Ms. Arnason joined the organization in 2001, assuming a leadership role in the research, development and implementation of the Cybertip.ca, the operation of the pilot project, and its roll out as a national service. Specifically, Ms. Arnason has played a key role in the development of the information technology that supports the service, the infrastructure for the operations and the design of its data collection system. Prior to joining Cybertip.ca, Ms. Arnason served on the executive management team of a number of private sector companies in the areas of information technology, human resource management and labour relations. Ms. Arnason has presented at the local, provincial and national level on the issue of child exploitation.

Jane Bailey (U of Ottawa, Law) is an assistant professor of law at the University of Ottawa Faculty of Law, Common Law Section. Her teaching interests include regulation of internet communications and cyberfeminism. Jane completed her LL.M. at the University of Toronto in 2002, supported by a Centre for Innovation Law and Policy scholarship. Before returning to legal studies, she practised civil litigation at Torys LLP in Toronto , where she acted as co-counsel on the first Canadian hate speech case before a Canadian Human Rights Tribunal. She also served as a law clerk to the Honourable Mr. Justice John Sopinka of the Supreme Court of Canada. Her written work focuses on technology's impacts on equality and free expression, including existing and forthcoming publications on the topics of internet hate speech, women's e-quality and the equality impacts of technology in the legal workplace. Her ongoing research focuses on the impact of evolving technology and inter-jurisdictional pressures relating to online hate, pornography and copyright on Canada's commitments to equality, freedom of expression, privacy and multiculturalism, as well as the societal and cultural impact of the Internet and emerging forms of private technological control, particularly in relation to members of socially disadvantaged communities.

David Butt (KINSA, ECPAT**)** is a trial and appellate lawyer with a wide ranging practice, and a leading expert and advocate in the fight against internet child exploitation. He was the first Canadian prosecutor to specialize in internet child abuse cases, and has since advised, consulted with, and taught prosecutors and police officers across the country. Building on his prosecutorial experience, Mr. Butt remains deeply involved in the fight against internet child exploitation. He has consulted throughout Europe, North America, South America and Asia. He donates many pro bono hours and countless media appearances to the issue. He sits on the Board of the Kids Internet Safety Alliance (KINSA) and is the Secretary of Bangkok based ECPAT International, the world's

largest NGO devoted exclusively to the fight against commercial sexual exploitation of children.

Corman Callanan (International Association of Internet Hotline Providers (INHOPE) – is CEO and past-president of INHOPE - the association of Internet Hotline Providers (www.inhope.org). The mission of Inhope is to facilitate and co-ordinate the work of Internet hotlines responding to illegal use and content on the Internet. Inhope has 20 member hotlines in 18 countries around the world. He was founding Chairman of the Internet Service Provider Association of Ireland (www.ispai.ie) and Secretary General of the European Service Provider Association (www.euroispa.org) until February 2003. He was founding Director of the Irish www.hotline.ie service responding to reports about illegal child pornography and hate speech on the Internet. In addition to representing INHOPE, he has represented the Irish and European Internet Service Provider's at Irish government and at EU level. Following work on international assignment in the USA and Japan , he established the first commercial Internet Services Provider business in Ireland in 1991 - EUnet Ireland - which was sold in 1996. He has presented seminars throughout Western, Central & Eastern Europe, the Middle East and Asia and has lectured on a wide range of technology issues for many years.

Paul Gillespie (Retired, Toronto Police Services) A former Toronto Police Services Detective Sergeant, Paul Gillespie established himself as an expert investigator during his 27 year career, particularly when it comes to criminals who abuse and exploit children. Paul spent his last 5 ½ years building and leading the Child Exploitation Section of the Toronto Police Service to become world leaders in this area. In 2003, Paul sent an email to Bill Gates, the founder and Chairman of Microsoft, to solicit his support in stopping the exploitation of children on the internet. Gates responded to Paul's passion and together, Paul and Microsoft collaborated to create CETS – the Child Exploitation Tracking System – which is now widely regarded as the most advanced investigative tool available to worldwide law enforcement. CETS is now being used by 30 different agencies in Canada and is being developed and deployed in countries all over the world, including the U.K., Indonesia, the U.S.A., Italy, Brazil, Spain and Chile. Paul retired from the Toronto Police Service in June of 2006 and continues to deploy CETS around the world and also to work with Kids Internet Safety Alliance, www.kinsa.net, a not for profit foundation.

Eric Heinze (Queen Mary, University of London, Law) is Reader in Law in the University of London, Queen Mary. He received his JD from Harvard Law School and his PhD from the University of Leiden (Netherlands), in addition to undergraduate and post-graduate study in the Universities of Paris (Licence, Maîtrise) and Berlin. His books include *The Logic of Constitutional Rights* (2005); *The Logic of Liberal Rights* (2003); *The Logic of Equality* (2003) and *Sexual Orientation: A Human Right* (Kluwer 1995) (Russian translation 2004), as well as an edited collection entitled *Of Innocence and Autonomy: Children, Sex and Human Rights* (Ashgate 2000) , and recent articles in the *Modern Law Review*, *Ratio Juris*, *The Michigan Journal of International Law*, and other major law journals. He has held major fellowships from the Fulbright foundation, the

French Government, and the German Academic Exchange Service. He has taught courses on Jurisprudence & Legal Theory, Constitutional Law, International Human Rights Law and Public International Law. His prior professional experience includes work for the International Commission of Jurists in Geneva and the United Nations Administrative Tribunal, and is a member of the Bars of New York and Massachusetts.

Patricia Holland has worked as a film editor and television producer. She is currently a writer and researcher in Media Studies, and a Senior Lecturer at the University of Bournemouth, UK. She specialises in television, popular culture and visual imagery, and is the author of *What is a Child?* London: Virago 1992 and *Picturing Childhood: the Myth of the Child in Popular Imagery* London: I.B.Tauris 2004. She has contributed articles to many books and journals, and her new article 'The child in the picture' will be published in the forthcoming *International Handbook of Children, Media and Culture* edited by Kirsten Drotner and Sonia Livingstone, London : Sage.

Earla-Kim McColl (RCMP – NCECC) is the Officer in Charge of the National Child Exploitation Coordination Centre (NCECC). Supt. McColl (E.K.) joined the RCMP in 1978. The majority of her service was spent in British Columbia in uniform policing. Her background also includes Victim Services and Sex Crimes. As a Corporal she was in charge of an Operational Audit Unit and as a Sergeant was i/c Internal Investigations. As a S/Sgt. she was a watch commander prior to coming to Ottawa the first time, as the NCO i/c Operational Policy. In this same position, she received her Commission and promotion to Inspector. She returned to operational policing as the Assistant Operations Officer for the Lower Mainland District of BC where a number of high profile services were integrated and operated seamlessly across municipal boundaries. E.K. was appointed the Officer in Charge of the National Child Exploitation Coordination Centre (NCECC) in September 2005. Her vision for the centre is to provide high level operational and strategic support to all operational units nationally and internationally; to concentrate on victim identification and rescue and to explore and exploit new technologies as they evolve. E.K. is the primary spokesperson for the NCECC. She is responsible for establishing and maintaining strategic partnerships both nationally and internationally. E.K. is the Canadian Lead on the Virtual Global Taskforce, a coalition of international law enforcement committed to eradicating child sexual exploitation.

Frédéric Mégret (McGill, Law) is an Assistant Professor of Law and the Canada Research Chair on the Law of Human Rights and Legal Pluralism. He holds a PhD in international law and relations from the University of Paris I and from the Graduate Institute of International Studies of the University of Geneva, and is a graduate of the Institut d'études politiques de Paris. Before joining the University of McGill, Professor Mégret was an Assistant Professor at the Faculty of Law of the University of Toronto . He has worked as a research associate at the European University Institute in Florence . Professor Mégret teaches and researches in public international law, international human rights law, and international criminal law.

Andrew Oosterbaan (U.S. Dept. of Justice, Child Exploitation and Obscenity Section) holds the Senior Executive Service position of Chief of the Child Exploitation and Obscenity Section (CEOS) for the United States Department of Justice. As Chief of CEOS, Oosterbaan manages a section of expert prosecutors and computer forensic specialists who conduct high-impact prosecutions, nationwide, involving child exploitation, child sex trafficking, and obscenity. CEOS also develops and coordinates multi-district investigations, law enforcement initiatives and operational strategies, and conducts an extensive training program for prosecutors, judges and law enforcement agents around the world. In recognition of his leadership, the Attorney General presented Oosterbaan with the John Marshall Award for Outstanding Legal Achievement for Participation in Litigation in August 2005. As Chief of CEOS, Oosterbaan regularly counsels Departmental leadership on critical policy matters in the areas of child exploitation and obscenity, and has been integrally involved in the drafting of major legislation targeting child exploitation, including the new Prosecutorial Remedies and Other Tools to End the Exploitation of Children Today Act of 2003 (the PROTECT Act), and the Adam Walsh Child Protection and Safety Act of 2006. Oosterbaan has also played a leading role in national efforts to identify victims of child pornography and to save them from further sexual abuse. The President recently honored Oosterbaan with the 2006 Presidential Rank Award for Meritorious Executive.

Christine Piper (Brunel University, UK) is a Professor in Brunel Law School, Brunel University, UK. She gained a First Class honours degree in History and taught in schools before undertaking Masters and Doctoral degrees in Sociology and Law and moving into academia. Her teaching and her research interests have covered family and child law, youth justice, sentencing and ADR, with a research focus on theorising around images of children in law and policy, the treatment of children in family and youth justice and the resolution of parental disputes. Prof. Piper was Case Commentaries editor for the *Child and Family Law Quarterly* during its first five years (1995-2000) and has since been a member of Editorial Board. She also jointly organised the Children and the Law Stream at the Annual Conferences of the UK Socio-legal Studies Association 2002-6 and co-convened the Child & Family and Sentencing & Punishment streams in April 2007.

Ethel Quayle (Dept. of Applied Psychology, University College Cork, Ireland) is a lecturer in the Department of Applied Psychology. University College Cork and a researcher and project director with the COPINE project. She trained as a clinical psychologist with a special interest in sexual offending and has focused for the last six years on victimisation of children through Internet abuse images. Recent research has led to the development of a CBT website for offenders and the development of guidelines for working with young people who engage in problematic sexual behaviour in relation to the new technologies. She is co-author of 'Child Pornography: An Internet Crime' (2003), Brunner and Routledge; 'Only Pictures? Therapeutic Approaches with Internet offenders' (2006) and 'Viewing Child Pornography on the Internet. Understanding the offence, managing the offender, helping the victims' (2005) both by Russell House Publishing, and has published in academic and professional journals.

Carol Rogerson (University of Toronto, Law) is a Professor at the Faculty of Law, University of Toronto, where she began teaching in 1983. She served as Associate Dean of the Faculty from 1991 to 1993. She holds degrees in law from Harvard and Toronto, and a master's degree in English from Toronto. Professor Rogerson's teaching and research interests encompass constitutional and family law, including children and the law. She is editor of *Competing Visions of Constitutionalism: The Meech Lake Accord* (with K. Swinton) and one of the co-authors of *Canadian Constitutional Law*. She is also the author of numerous law review articles in both the constitutional and family law areas and has frequently worked with governments on issues of family law reform.

Bruce Ryder (Osgoode Hall Law School, York) is an Associate Professor at Osgoode Hall Law School where he has taught since 1987 after clerking for Justice Gerald Le Dain of the Supreme Court of Canada (1984-85), and after receiving an LL.M. from Columbia University (1987) and an LL.B. from the University of Toronto (1984). He is currently the Director of the Centre for Public Law and Public Policy at York University, and the Treasurer of the Canadian Law and Society Association. He served as Editor-in-Chief of the Osgoode Hall Law Journal from 1997-2000, and has taught courses in Public Law, Constitutional Law, Canadian Federalism, Torts, Sexuality and the Law, Discrimination and the Law, and Freedom of Expression. His current research focuses on equality rights, religious freedom, the legal regulation of conjugal relationships, and the censorship of sexual expression. He worked closely with the Law Commission of Canada on the preparation of their report *Beyond Conjugality: Recognizing and Supporting Close Personal Adult Relationships* (2001). Recent publications include "The Canadian Conception of Equal Religious Citizenship" in Richard Moon ed., *Religion and Citizenship* (forthcoming, UBC Press, 2007); "The End of Umpire? Federalism and Judicial Restraint", (2006) 34 S.C.L.R. (2d); "State Neutrality and Freedom of Conscience and Religion", (2005) 29 S.C.L.R. (2d) 169; "What Is *Law* Good For? An Empirical Review of Equality Rights Decisions", (2004) 24 S.C.L.R. (2d) 103; "Suspending the Charter", (2003) 21 S.C.L.R. (2d) 267; "The Harms of Child Pornography Law" (2002) 36 U.B.C. L. Rev.; "What is Marriage-Like Like? The Irrelevance of Conjugality", (2001) Can. J. Fam. Law 289 (with Brenda Cossman); and "The *Little Sisters* Case, Administrative Censorship and Obscenity Law", (2001) 39 Osgoode Hall L.J. 207.is an Associate Professor at Osgoode Hall Law School , where he is Director of the Centre for Public Law and Public Policy. His research and publications focus on a range of contemporary constitutional issues, including those related to federalism, equality rights, freedom of expression, Aboriginal rights, and Quebec secession. He has also published articles that explore the historical evolution of constitutional principles and is currently researching the history of book censorship in Canada.

Dr. Michael Seto is a psychologist with the Law and Mental Health Program at the Centre for Addiction and Mental Health in Toronto, and an Associate Professor in the Department of Psychiatry and at the Centre of Criminology at the University of Toronto. Dr. Seto has published extensively on pedophilia and sexual offending and regularly presents at scientific meetings and professional workshops on these topics. His main

research interests are pedophilia; sexual offending against children; child pornography offending; risk assessment; psychopathy; and program evaluation.

Andrea Slane (Centre for Innovation Law and Policy, University of Toronto, Law) is the Executive Director of the Centre for Innovation Law and Policy at the University of Toronto, Faculty of Law. She co-chaired the Centre's 2005 Symposium on Online Child Exploitation, and authored the Centre's recommendations that came out of those proceedings. She has published on such topics as the personal privacy expectations violated by unsolicited bulk email and the Canadian Human Rights Tribunal's handling of the technological features of the Internet in online hate complaints. Before joining the Faculty of Law in 2006, Andrea practiced trade-mark, copyright, privacy and technology law. She obtained her JD from the University of Toronto in 2003, and a PhD in Comparative Literature from the University of California, San Diego in 1995. Prior to attending law school, she was an Assistant Professor of Literature and Film at Old Dominion University in Norfolk, Virginia, and authored *A Not So Foreign Affair: Fascism, Sexuality and the Cultural Rhetoric of American Democracy* (Duke University Press, 2001).

Janis Wolak (Crimes Against Children Research Center, University of New Hampshire, USA) is a Research Assistant Professor at the Crimes Against Children Research Center of the University of New Hampshire . She has a B.A. in Sociology from New College in Sarasota, Florida , a law degree from Southwestern University School of Law, and a M.A. in Sociology from the University of New Hampshire . She is a director of the first Youth Internet Safety Survey and a co-Principal Investigator of the second Youth Internet Safety Survey, the first and second National Juvenile Online Victimization Studies and the National Juvenile Prostitution Study. She is the author and co-author of numerous articles about child victimization, Internet-related sex crimes, and youth Internet use.

Appendix B:

Roundtable Discussion Participants

May 8, 2007, University of Toronto

David Butt, Barrister and Legal Director of the Kids' Internet Safety Alliance

Vicky Kuek, Research Fellow, Centre for Innovation Law and Policy

Liz Lambert, Research Assistant to Faye Mishna, Faculty of Social Work, University of Toronto

Bruce Ryder, Associate Professor, Faculty of Law, Osgoode Hall Law School

Andrea Slane, Executive Director, Centre for Innovation Law and Policy

Appendix C:

Summary of Recommendations Made in the White Paper of 2005

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.

b) 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[1] 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.

[1] 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".

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 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) Police training regarding online meeting crimes:

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) Police training regarding child pornography

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) Special prosecutors:

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) Collaboration with industry:

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.

3. **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:

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

ii. ISPs should help in publicizing the national tipline, cybertip.ca, to subscribers.

iii. 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:

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

ii. 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.

iii. 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) Legislative reform:

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) Incentives for development of technical tools:

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.

4. **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.

Appendix D:

Civil Action Sections of South Dakota Title 22, Chapter 24A

SOUTH DAKOTA CODIFIED LAWS
CHAPTER 22-24A

CHILD PORNOGRAPHY

22-24A-7. Liability for civil damages. Any person, except a minor, who knowingly participates in any conduct proscribed by §§ 22-19A-1, 22-24A-1 to 22-24A-20, inclusive, 22-24B-1, 23A-27-14.1, and 43-43B-1 to 43-43B-3, inclusive, is liable for civil damages.

22-24A-8. Persons who may bring action for damages. Any of the following persons may bring an action for damages caused by another person's conduct as proscribed by §§ 22-19A-1, 22- 24A-1 to 22-24A-20, inclusive, 22-24B-1, 23A-27-14.1, and 43-43B-1 to 43-43B-3, inclusive:

(1) The child;

(2) Any parent, legal guardian, or sibling of a victimized child;

(3) Any medical facility, insurer, governmental entity, employer, or other entity that funds a treatment program or employee assistance program for the child or that otherwise expended money or provided services on behalf of the child;

(4) Any person injured as a result of the willful, reckless, or negligent actions of a person who knowingly participated in conduct proscribed by §§ 22-19A-1, 22-24A-1 to 22-24A-20, inclusive, 22-24B-1, 23A-27-14.1, and 43-43B-1 to 43-43B-3, inclusive.

If the parent or guardian is named as a defendant in the action, the court shall appoint a special guardian to bring the action on behalf of the child.

22-24A-9. Persons from whom damages may be sought. Any person entitled to bring an action under § 22-24A-8 may seek damages from any person, except a minor, who knowingly participated in the production or in the chain of distribution of any visual depiction proscribed by §§ 22-19A-1, 22-24A-1 to 22-24A-20, inclusive, 22-24B-1, 23A-27-14.1, and 43-43B-1 to 43-43B- 3, inclusive.

22-24A-10. Damages recoverable. Any person entitled to bring an action under § 22-24A-8 may recover all of the following damages:

(1) Economic damages, including the cost of treatment and rehabilitation, medical expenses, loss of economic or educational potential, loss of productivity, absenteeism, support expenses, accidents or injury, and any other pecuniary loss proximately caused by the proscribed conduct;

(2) Noneconomic damages, including physical and emotional pain, suffering, physical impairment, emotional distress, mental anguish, disfigurement, loss of enjoyment, loss of companionship, services, and consortium, and other nonpecuniary losses proximately caused by the proscribed conduct;

(3) Exemplary damages;

(4) Attorneys' fees; and
(5) Disbursements.

22-24A-13. Statute of limitations. Any action for damages under §§ 22-19A-1, 22-24A-1 to 22-24A-20, inclusive, 22-24B-1, 23A-27-14.1, and 43-43B-1 to 43-43B-3, inclusive, shall be commenced within six years of the time the plaintiff knew, or had reason to know, of any injury caused by violations of §§ 22-19A-1, 22-24A-1 to 22-24A-20, inclusive, 22-24B-1, 23A-27-14.1, and 43-43B-1 to 43-43B-3, inclusive. The knowledge of a parent, guardian, or custodian may not be imputed to the minor.

For a plaintiff, the statute of limitations under this section is tolled while any potential plaintiff is incapacitated by minority.

22-24A-14. Civil action stayed pending completion of criminal action --Statute of limitations tolled. On motion by a governmental agency involved in an investigation or prosecution, any civil action brought under §§ 22-19A-1, 22-24A-1 to 22-24A-20, inclusive, 22-24B-1, 23A-27-14.1, and 43-43B-1 to 43-43B-3, inclusive, shall be stayed until the completion of the criminal investigation or prosecution that gave rise to the motion for a stay of the action. The statute of limitations as provided in § 22-24A-13 shall be tolled for the time any such stay is in effect.