



## ***THERE OUGHT TO BE A LAW: PROTECTING CHILDREN'S ONLINE PRIVACY IN THE 21ST CENTURY***

A Discussion paper for Canadians by the Working Group of Canadian Privacy Commissioners and Child and Youth Advocates

November 19, 2009

## Contents

Acknowledgments.....	3
Introduction.....	5
The Working Group .....	7
A Child's Right to Privacy and the Risks Online .....	8
Potential Dangers: Online Commercial Exploitation of Children .....	8
Potential Dangers: Online Child Sexual Exploitation.....	10
Potential Dangers: Online Invasion of Privacy .....	12
Options for Law Reform .....	13
Specialised Legislation Protecting Children's Online Privacy: the US COPPA model .....	13
General Legislation prohibiting marketing aimed at minors:.....	14
The Quebec Consumer Protection Model.....	14
Prohibiting commercialization of children's online play spaces.....	15
Non-Commercial Online Play Spaces.....	16
Law Reform to PIPEDA.....	17
Requirements for Internet Service Providers .....	18
Mandatory Reporting of Child Pornography.....	21
Safeguarding against the distribution of prohibited internet sites .....	23
Children's Privacy as a Human Right .....	23
Conclusion.....	25
Appendix I - Summary of Legislative Reform Proposals.....	28

## Acknowledgments

Everyone as a child has heard the stories of children tempted to run away and join the circus. The lure of adventure and fame is engrossing for every child. Today a vast virtual world of adventure entreats our children and poses new risks to their privacy, the security of their persons and their healthy development. The working group of child and youth advocates and information and privacy commissioners was formed in January of this year to commence a dialogue and launch a public debate on the legislative parameters that can and should help parents navigate the net and ensure that all its potential is made available to their children without undue risk to their privacy or their safety.

This collaboration between offices with varying mandates affecting children's rights augurs well, I think, for improved enforcement of the rights guaranteed under the *Convention on the Rights of the Child* in Canada. The main goal of the working group, to produce a discussion paper aimed at informing public debate around the need for legislative reform in the area of children's privacy, was at once modest and realistic. The goal could not have been achieved however without significant collaboration and contributions on several fronts.

I want to thank first and foremost the numerous members of the working group who participated at various stages in this process, including from the privacy oversight officers table, Diane Aldridge from the Saskatchewan IPC office, Kasia Krzymien from the Office of the Privacy Commissioner of Canada, Fakhri Gharbi, from the Commission de l'accès à l'information du Québec and Suzanne Hollett from the IPC office in Newfoundland and Labrador. From the Canadian Council of Provincial Child and Youth Advocates I would like to acknowledge the contributions of John Greschner from the BC Representative for Children and Youth Office, John Mould, the CYA for Alberta and Christine Brennan, Child and Youth Services Coordinator for the Nova Scotia Ombudsman's Office. A deep expression of thanks is due also to the several experts and panelists who took part in our Working Group meetings and presented at our symposium in Fredericton last May, including, Professor Valerie Steeves of the University of Ottawa, John Lawford with the Public Interest Research Group, Parry Aftab, a New York-based children's Internet lawyer, Signy Arnason with the Canadian Centre for Child Protection in Winnipeg, Paul Gillespie of the Kids Internet Safety Alliance and Jason Doiron of the Fédération des Jeunes Francophones du Nouveau-Brunswick. All of these contributions are included in the report which follows which was compiled through the efforts of several members of my staff, including Christian Whalen, our legal counsel who chaired the Working Group and Jessica West and Kara Patterson who had a lead role in crafting the text but who were helped in great measure also by Jennifer Murray, Ben Reentovich, Maria Montgomery and Janel Guthrie.

Finally, I wish to acknowledge the broad support and encouragement I have received from colleagues federally and provincially at both the Child and Youth Advocates table and the Information and Privacy Commissioners table for this work. The report will bear fruit in direct relation to the uses and good offices to which my colleagues can put it in their own respective jurisdictions. For this too, I am most grateful.

Bernard Richard

Ombudsman and Child and Youth Advocate

## **Introduction**

Privacy is the ability of an individual or group to seclude themselves or information about themselves thereby revealing themselves selectively. The boundaries and content of what is considered private differ among cultures and individuals.

As technology has advanced, the way in which privacy is protected and violated has changed with it. The increased ability to collect information in a networked environment has led to new ways in which privacy can be breached. Privacy laws must be adapted to reflect the changes in technology in order to address these issues and maintain people's right to privacy, including the ability to control what information one reveals about oneself over networks and to control who can access that information.

Privacy is important to children because it allows them to control how much and when they reveal information about themselves. This is an important factor in the natural development of children, because privacy is linked to the formation of identity and the ability to enter into healthy relationships with others.

Today's children are growing up in a wired world and that fact poses significant challenges for privacy protection. Canadian children are among the most wired in the world. All public schools in Canada have been wired to the Internet since 1997. In 2003, almost 75% of households with children were connected to the Internet.<sup>1</sup> Today, residential numbers have approached universal access, equivalent to cable and phone penetration.

Although early attempts to wire children were based on the premise that it would help them learn and acquire job-related skills, children primarily use the Internet as social networking tool. Social networking programs like MSN Messenger, Facebook, and YouTube have millions of users worldwide, many of whom are children and adolescents. Canadians lead the world in terms of their per capita adoption of these technologies and young Canadians continue to lead the charge by a very wide margin.

Along with its incredible potential, the Internet and its increasingly portable devices can present many risks to children and young people if they are misused, for instance as a result of cyber-bullying, grooming, privacy violations or exposure to harmful content (pornography, racism, etc). The Internet has also facilitated an explosion of online child sexual exploitation, which raises a number of additional privacy concerns for the child subjects of sexual abuse footage that has been posted online. While online commercial exploitation and online sexual exploitation of children are fundamentally different in nature and in the harms that each pose to children, both forms of online exploitation clearly violate the privacy interests of children.

---

<sup>1</sup> Statistics Canada, *Household Internet Use Survey, 2003* (8 July 2004), <<http://www.statcan.ca/Daily/English/040708/d040708a.htm>>.

A number of initiatives to combat online child sexual exploitation have been launched in Canada, including the Canadian Centre for Child Protection (“C3P”), a charitable organization dedicated to the personal safety of children. In 2002, C3P set up Cybertip.ca, a national tip line for reporting online sexual exploitation of children.<sup>2</sup> The federal government also launched a national strategy with the Royal Canadian Mounted Police in 2004 that included the creation of the National Child Exploitation Coordination Centre.<sup>3</sup> While these initiatives are laudably targeting the proliferation of online sexual exploitation of children, there remains much work to be done to address the ongoing privacy issues that victims endure.

Less attention has been given to online commercial exploitation of children, and privacy commissioners and data protection authorities have been among the first to raise concerns about the associated risks. In June 2008, Canada’s privacy commissioners established the Regina Resolution,<sup>4</sup> an education-based approach that encouraged the cooperation and partnership among commissioners, governments, industry and organizations to improve online privacy for children and young people. They agreed to work together to implement public education activities to increase awareness among children and young people to the privacy risks inherent to their online activities.

In the fall of 2008, the Strasbourg Resolution was created at the 30<sup>th</sup> International Conference of Data Protection and Privacy Commissioners.<sup>5</sup> The resolution encouraged countries to work together and devote effort and resources to the matter of children’s online privacy in each of their respective jurisdictions. It acknowledged that while many young people recognize the risks associated with their online activities, they often lack the experience, technical knowledge and tools to mitigate those risks.

## **The Working Group**

The focus of the both the Regina and Strasbourg Resolutions was to do more to educate ourselves and young people and their parents about online privacy. Public awareness and education will help but stronger laws are also needed. The Children’s Online Privacy Working Group has been working to identify and devise new legislative standards to better protect children’s online privacy.

The Children’s Online Privacy Working Group, began its work in January 2009 on the initiative of Canadian provincial child and youth advocates and privacy commissioners. Comprised of a representative number of commissioners and advocates from across the country, the Working Group looked at the issue of children’s online privacy through

---

<sup>2</sup>Cybertip.ca: <<http://www.cybertip.ca>>.

<sup>3</sup> National Child Exploitation Coordination Centre, online: Royal Canadian Mounted Police: <<http://www.rcmp-grc.gc.ca/ncecc-cncee/>>.

<sup>4</sup> Children’s Online Privacy: Resolution of Canada’s Privacy Commissioners and Privacy Oversight Bodies, online: Privacy Commissioner of Canada: <[http://www.priv.gc.ca/media/nrc/2008/res\\_080604\\_e.cfm](http://www.priv.gc.ca/media/nrc/2008/res_080604_e.cfm)>.

<sup>5</sup> Resolution on Children’s Online Privacy, online: 30<sup>th</sup> International Conference of Data Protection and Privacy Commissioners: <[http://www.privacyconference2008.org/adopted\\_resolutions/STRASBOURG2008/resolution\\_child\\_privacy\\_en.pdf](http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_child_privacy_en.pdf)>.

the dual lenses of the commercialization of children's online space, including advertising directly to children and the use of children's online space for commercial data-mining purposes, and protecting children from the dangers of the Internet, including child pornography, exploitation and luring. The Working Group also explored the emerging risks to children's privacy posed by misuse of social networking sites, cyber-bullying, sexting and online defamation.

The primary goal of the Working Group was to produce this discussion paper which was presented in draft form at the September annual meeting of the Canadian Council of Provincial Child and Youth Advocates ("CCPCYA") and the September summit of Information Privacy Commissioners ("the Commissioners"). The Working Group has collected the feedback from these forums to release a revised discussion paper in anticipation of National Child Day, November 20<sup>th</sup>, 2009, which also marks this year the 20<sup>th</sup> anniversary of the signing of the UN Convention on the Rights of the Child.

The Working Group was formed in the late fall of 2008 and early part of 2009 as a follow up to Professor Valerie Steeves' presentations in Regina and Ottawa to annual meetings of Commissioners and Advocates. Advocates' offices from Nova Scotia, Alberta and BC have taken part, as have Commissioners' offices in Saskatchewan, Ottawa, Quebec and Newfoundland. The New Brunswick Office of the Ombudsman and Child and Youth Advocate, which is common to both forums, has chaired the Working Group. A number of leading researchers in the area of children's online privacy have participated and assisted the Working Group's deliberations. Following a few conference calls early in 2009, sharing of best practices legislatively and devising a plan of action, the Working Group met for a two day seminar in Fredericton, New Brunswick. This paper summarizes and outlines some of the legislative provisions discussed during the seminar, as options for further study and law reform. Much of the discussion in Fredericton focused on identifying the harms and determining whether constitutional, statutory or social norms would be most effective in addressing them. Before looking more closely at existing and proposed legislative models, we start by summarizing the discussion related to the harms in question.

## **A Child's Right to Privacy and the Risks Online**

### **Potential Dangers: Online Commercial Exploitation of Children**

Children see the Internet as a place to play and socialize, and the vast majority of their activities take place on commercial sites that are designed to generate a profit. The harm as it relates to the commercialization of online space is not immediately clear. Children are lured to these websites by games, contests, and the opportunity to communicate with their peers. These sites collect marketing information from its users by collecting data provided by the user when they participate in online quizzes or games which record the user's likes and dislikes. This information is then used to select products to advertise to children that are specifically aligned with their expressed preferences. The result is a form of social sorting whereby large corporations have too great an influence over the play spaces of children and youth. This seamless blend of commercial content, entertainment and play on children's sites also provides an

opportunity to disguise marketing as empowerment. What has transpired—the unrestrained gathering and use of children’s personal information with no clear limits on how that data can be used, retained, or transferred—is of significant concern.

Commercial content is embedded not only into virtual spaces, but also into virtual relationships that work to integrate brands into a child’s identity. Websites such as Barbie.com do not focus so much on collecting marketing data but rather encourage children to buy their product by developing a personalized relationship between the child and the product. The product is often personified in a way that relates to the child. The child, for example, may be able to communicate directly with Barbie. By having children identify with a product, the company is better able to engage the child and to groom them into loyal consumers from an early age.

This kind of marketing may be analyzed as an invasion of privacy if the corporation penetrates the child’s private spaces and extracts data for instrumental purposes by manipulating the child communicatively. For instance the child may not be situated as a consumer interacting with a salesperson but rather as a friend talking to a ‘friend.’ Part of the value of privacy in the past was that it limited the circulation of recorded judgments about individuals, leaving them free to seek self-realization in an open environment. Today, unbeknownst to the user, information is recorded and judgments are used against the user to solidify his or her preferences.

Young children typically cannot differentiate between online content and advertising and do not understand the consequences of revealing their personal information to marketers. Amongst other articles, the Convention on the Rights of the Child provides for a child’s right to privacy (Article 16), but also recognizes the important role that mass media plays in children’s lives (Article 17) and that every child should have the freedom to seek ideas through media of his or her choice (Article 13). These provisions go beyond questions of access and seek to ensure that media will promote a child’s social and moral well-being.

Access to the Internet now plays a large role in the development of children and adolescents. Older children tend to use the Internet to obtain independence from their parents and families, to communicate with their peers, to try on new identities, and to exercise their freedom of expression by articulating their opinions. Many adolescents view social networking tools as a way to maintain a protective distance from the person they are communicating with, which enables them to think more about what they are going to say and avoid embarrassing situations that would occur on the telephone or in a face-to-face conversation.

Furthermore, as technology continues to expand, one must remember that Internet access is not limited to availability through computers. Most of today’s mobile phones provide access to the Internet, and due to their compact size and portability, provide the ability to be connected to the outside world all the time. The newest generation of mobile phones, smartphones, continues to grow in popularity. Many smartphone plans



include unlimited access to trendy networking websites to keep children and youth constantly connected to these sites.

These forms of targeted marketing of children rely heavily on manipulation to extract personal information to promote the commercial interests of the corporation, reaping hefty financial profits at the expense of children's dignity, autonomy, and privacy interests.

Advances in mobile phone technology and the widespread use of mobile phones by children and youth have enabled new forms of social interaction, some of which are disturbing. Mobile phones are now embedded with cameras and have the capability to send photographs, videos, and messages that the user creates. There has been a great deal of concern raised by the growing tendency of some young people to send photos, videos, and messages with explicit sexual content, called sexts, over their mobile phones. A social danger with sexting is that material that was intended by the sender to be private can very easily be widely promulgated, over which the originator has no control. The phenomenon also raises interesting questions about the relationship between privacy, technology and media representations of youth.

In the United States, child pornography criminal charges have been laid against teenagers who have sent sexually explicit photographs to others. However, states such as Vermont have felt that harsh criminal laws for child pornography are not the proper way to deal with this problem. Instead, they have taken action to prevent such charges from being laid by introducing a bill to legalize the consensual exchange of graphic images between two people aged thirteen to eighteen years old.<sup>6</sup> Passing along such images to others would remain a crime.

Online play space has become a omnipresent element of childhood and more work needs to be done in terms of how children and youth access the Internet and what is done with the data collected by third parties. In both cases serious violations of a child's right to privacy occur and a stronger guarantee of a child's right to privacy may provide the best analytical framework for tackling these emerging social problems in the information age.

### **Potential Dangers: Online Child Sexual Exploitation**

Sexual exploitation of children is a gross violation of their right to respect for their human dignity and physical and mental integrity. Fulfillment of the states' human rights obligations under international law requires effective protection for all children from all forms of sexual exploitation. The Convention on the Rights of the Child affirms the status of all children as equal holders of human rights and empowered actors in the realization of their rights, and it includes explicit rights to protection from all forms of violence and exploitation, including sexual exploitation.

---

<sup>6</sup> *An Act Relating to Expanding the Sex Offender Registry*, VT LEG 247571.1 (2009) Sec. 4. 13 V.S.A. § 2802b.

While technology forges ahead at a breakneck pace, law enforcement has not been able to keep pace with the growth in Internet-facilitated criminal activity, and the widespread use of the Internet has greatly contributed to and facilitated the sexual exploitation of children via electronic means. Child sexual abusers and predators have greater and easier access to children through ever-expanding means of online communication—e-mail, instant chat programs such as MSN Messenger, interactive gaming sites with chat capabilities, and social networking websites like Facebook, to name but a few. Further, electronic devices and the Internet have greatly facilitated the distribution, if not the production, of child pornography. Each of these raises unique privacy concerns for children.

In 2002, the Criminal Code was amended to create the criminal offence of luring.<sup>7</sup> People who engage in online child luring take advantage of children sharing their personal information online. Using personal information that a child has posted online, lurers forge a “bond” with the child and gradually steer conversation topics to those of a sexual nature, which may include sharing online pornographic material, as part of the grooming process. These conversations can quickly escalate to the lurer pressuring the child to meet, with the express or intended aim of engaging in sexual activity with the child. The issue of luring is one that has a greater impact on adolescents as they are exposed to potential predators when they enter the online world, and there is evidence that exposure to sexualized content is one of the steps in the process of grooming a young person for an assault. The issues become ever more complicated in a world where mainstream media images are increasingly eroticizing children and teenagers.

Another issue surrounding the widespread use of the Internet is that it has facilitated the online sharing and distribution of child pornography. The Internet is being used as a medium to send images and video around the world of actual children being exploited and abused. Not only are children being increasingly sexualized, there is also a concern that there may be a link between viewing online material and committing real world assaults.<sup>8</sup>

The particular ways in which harm might arise from the possession of abusive images were summarized by the Supreme Court of Canada in *R. v. Sharpe*:

1. Child pornography promotes cognitive distortions such that it may normalize sexual activity with children in the mind of the possessor, weakening inhibitions and potentially leading to actual abuse.
2. Child pornography fuels fantasies that incite offenders.

---

<sup>7</sup> *Criminal Code of Canada*, R.S.C., 1985, c. C-46, s. 172.1. The scope of the provision is currently under scrutiny by the Supreme Court of Canada, which will determine whether targeting children online for sexual conversations where there is no intent to meet and no sexual activity has taken place meets the criteria outlined in the luring provision: *Craig Bartholomew Legare v. Her Majesty the Queen*, Judgment October 15, 2009. On appeal from the Court of Queen’s Bench of Alberta, 2006 ABQB 248.

<sup>8</sup> See <http://www.cybertip.ca/app/en/risks> for a list of risks to children on the Internet.

3. Prohibiting the possession of child pornography assists law enforcement efforts to reduce the production, distribution and use that result in direct harm to children.
4. There is 'clear and uncontradicted' evidence that child pornography is used for grooming and seducing victims.
5. To the extent that most child pornography is produced using real children, the viewer is in a sense an accessory after the fact to an act of child abuse by providing a market for it.<sup>9</sup>

The harm inflicted on children who are subjects of child pornographic materials is obvious. Sexual abuse is in itself a gross violation of a child's dignity and security of the person. Where the abuse is recorded and shared with others for pornographic purposes, victims are in the position of being re-abused every time the recordings are viewed. Digital technology and the Internet have ensured that recordings posted online become a permanent, irretrievable, and indestructible record that perpetuates the abuse every time it is viewed, copied, and distributed. The Supreme Court of Canada recently recognized the severity and continuous nature of the harm of online child pornography, and the need to impose strict sentences on offenders given the nature of this harm:

I note that L.M. disseminated his pornography around the world over the Internet. The use of this medium can have serious consequences for a victim. Once a photograph has been posted on the Web, it can be accessed indefinitely, from anywhere in the world. R.M. will never know whether a pornographic photograph or video in which she appears might not resurface someday.<sup>10</sup>

The privacy interests of children at stake regarding online child pornography are different in that they arise in the context of a permanent digital record of abuse that can be reproduced electronically indefinitely. Once an image or recording is posted online, it effectively becomes a permanent public record, with no controls to restrict when, where or how often it is distributed. What steps can be taken to minimize the impact of such a gross, ongoing and permanent violation of a child's privacy and dignity?

While the primary focus has been and must continue to be to work towards reducing the production and distribution of child pornography, investigation, prosecution, and prevention processes and strategies raise their own privacy concerns for the children involved. Steps must be taken to ensure that a minimum amount of people have access to child pornography throughout the law enforcement and legal process. The RCMP and Cybertip.ca maintain databases of known child pornographic content and lists of websites that contain illegal content, and under the current voluntary system, Cleanfeed provides encrypted lists to participating ISPs which in turn upload the encrypted lists to their routers to block subscriber access. While this current system has not yet been subject to a security breach, the option of legally requiring all ISPs to

---

<sup>9</sup> *R. v. Sharpe*, 2001 SCC 2.

<sup>10</sup> *R. v. L.M.*, 2008 SCC 31 at para. 28. L.M. was convicted of sexually assaulting his daughter and of making, distributing and possessing child pornography. The Court upheld the trial judge's imposition of the maximum 15-year sentence, overruling the Court of Appeal's ruling to reduce the sentence to 9 years.

participate would raise additional privacy concerns regarding the security of the information, and a security breach with this kind of highly sensitive information would be disastrous.

The online sexual exploitation of children presents immediate and long-term harm to children, who often in turn repeat the cycle of abuse in a myriad of ways, making this a matter of pressing societal concern. Stronger guarantees of children's right to privacy, greater privacy protections for victims of online sexual exploitation, and legislative reforms to better combat Internet-facilitated criminal activities that target children must be considered.

### **Potential Dangers: Online Invasion of Privacy**

Another cause for concern with the advent of social media and the seemingly limitless ability to post and update Facebook pages and blogs is how children and adults alike represent others online. Repeating rumours about others or posting photographs of others without their permission can easily happen with little malicious intent, but this could be construed as an invasion of privacy, raising the risk of civil liability for libel, defamation, and other torts against a person's reputation. It cannot be stated too often that what is posted online essentially becomes a permanent, irretrievable public record that can have far-reaching consequences beyond what was intended when originally posted:

The Internet represents a communications revolution. It makes instantaneous global communication available cheaply to anyone with a computer and an Internet connection. It enables individuals, institutions, and companies to communicate with a potentially vast global audience. It is a medium which does not respect geographical boundaries. Concomitant with the utopian possibility of creating virtual communities, enabling aspects of identity to be explored, and heralding a new and global age of free speech and democracy, the Internet is also potentially a medium of virtually limitless international defamation.<sup>11</sup>

Misappropriation of personality and impersonation of others are also torts that are greatly facilitated by the development of new technologies.

Courts across Canada have been increasingly hearing claims of online libel and defamation, and there is an emerging trend of findings of legal liability for these actions.<sup>12</sup> A recent court decision took this further and found that there is no reasonable expectation of privacy regarding the use of the Internet for the purpose of publishing defamatory statements and provided a civil remedy for the ISPs to disclose the names of customers to identify the proper defendants in an action for libel.<sup>13</sup> The veil of

---

<sup>11</sup> Matthew Collins, *The Law of Defamation and the Internet* (Oxford University Press, 2001), at para. 24.02.

<sup>12</sup> *WeGo Kayaking Ltd. et al v. Sewid, et al*, 2007 BCSC 49; *Henderson v. Pearlman*, 2009 CanLII 43641 (ON S.C.).

<sup>13</sup> *York University v. Bell Canada Enterprises*, 2009 CanLII 46447 (ON S.C.).

anonymity on the Internet will not shield people from legal responsibility for their actions online.

Today's reality is that the online world is becoming an increasingly important aspect in the lives of children and youth; they play, communicate and do school work online. It is no longer enough to put the onus completely on parents and schools to limit the ability of children and youth to access the Internet. The government must be pressed to recognize that protection of children's online privacy is a human rights concern, and laws must be put in place to regulate the collection and use of this data.

## Options for Law Reform

### **Specialised Legislation Protecting Children's Online Privacy: the US COPPA model**

Technology is changing our societies so fast that it is difficult for legislators to keep up. In 1998 the United States enacted the *Children's Online Privacy Protection Act of 1998* ("COPPA") to address the issue of the online privacy of children.<sup>14</sup> This legislation applies to operators of commercial websites directed at children that collect personal information from children under the age of thirteen. The legislation requires that the website operators obtain "verifiable" parental consent before collecting information from a child.<sup>15</sup> Typically, this means that the operator must make reasonable efforts to provide a parent with notice of its information collecting practices and ensure that a parent consents to the collection of the information on that basis. However, the Federal Trade Commission states that "if the operator uses the information for internal purposes, a less rigorous method of consent is required. If the operator discloses the information to others, the situation presents greater dangers to children, and a more reliable method of consent is required."<sup>16</sup> Internal purposes include "marketing back to a child based on his or her preferences or communicating promotional updates about site content."<sup>17</sup>

The problem is that *COPPA* has been ineffective in protecting the invasion of online privacy of children. One of the issues is that there is no way to verify the parental consent. Website privacy policies are often so difficult to understand that no one is clear what they are consenting to. Furthermore, most children (and adults) fail to read privacy policies before giving their consent.

*COPPA* defines "personal information" as:

- (8) PERSONAL INFORMATION.—The term "personal information" means individually identifiable information about an individual collected online, including—  
(A) a first and last name;

---

<sup>14</sup> 15 U.S.C. ss. 6501–6506 (2000), <<http://uscode.house.gov/download/pls/15C91.txt>> [COPPA].

<sup>15</sup> US, Federal Trade Commission, *How to Comply with the Children's Online Privacy Protection Rule*, <<http://www.ftc.gov/bcp/online/pubs/buspubs/coppa.htm>>.

<sup>16</sup> *Ibid.* at 2.

<sup>17</sup> *Ibid.* at 1.

- (B) a home or other physical address including street name and name of a city or town;
- (C) an e-mail address;
- (D) a telephone number;
- (E) a Social Security number;
- (F) any other identifier that the Commission determines permits the physical or online contacting of a specific individual; or
- (G) information concerning the child or the parents of that child that the website collects online from the child and combines with an identifier described in this paragraph.

*COPPA* only requires consent for information that can specifically identify an individual child; its wording is such that it does not cover non-personal information or aggregate data. It is, in part, due to these limitations that it is not considered an effective model as it still allows for behavioural targeting. Interestingly some U.S. Congress representatives are now considering legislative proposals that would ban behavioural targeting of children altogether.<sup>18</sup> If the US moves in this direction it will make it much easier to enforce similar legislative developments in Canada.

## **General Legislation prohibiting marketing aimed at minors**

### **The Quebec Consumer Protection Model**

Another piece of legislation aimed at protecting children from the influence of advertisers is the Quebec *Consumer Protection Act*.<sup>19</sup> This Act, enacted in 1987, has banned any advertising directed at children under the age of thirteen. The regulations passed pursuant to the *Act* contain a rather complex scheme of exemptions.<sup>20</sup> While this Act does not consider the issues of online privacy or data-management, it does provide an example of how commercial activities have been limited to protect children's interests. The general view taken by the Quebec legislature and supported by Canadian courts is that under the age of thirteen children are particularly susceptible to the manipulative content of advertising campaigns.

Quebec's Consumer protection provisions were first made famous in Canadian legal circles when Irwin Toy contested their validity before the Supreme Court of Canada. The constitutionality of limiting this type of commercial advertising was upheld by the Supreme Court of Canada in *Irwin Toy Ltd. v. Quebec (Attorney General)*.<sup>21</sup> Although such legislation was found to be an infringement on the freedom of expression, the law was upheld because of the pressing and substantial objective of the protecting a group that is vulnerable to commercial manipulation. The majority of the Court felt that children

---

<sup>18</sup> See press report: <http://mediadecoder.blogs.nytimes.com/2009/09/01/privacy-advocates-push-for-new-legislation/> .US Privacy Advocates have released this month a legislative primer demanding law reform to protect children from behavioural targeting: <http://www.uspirg.org/uploads/s6/9h/s69h7ytWnmbOJE-V2uGd4w/Online-Privacy---Legislative-Primer.pdf> .

<sup>19</sup> *Consumer Protection Act*, R.S.Q. 1987, P-40.1, ss. 248, 249, 364.

<sup>20</sup> Regulation Respecting the Application of the Consumer Protection Act, R.S.Q. c. P-40.1, r. 1, (ss. 87 to 91).

<sup>21</sup> *Irwin Toy Ltd. v. Quebec (Attorney General)*, [1989] 1 S.C.R. 927.

are not as able as adults to evaluate the persuasive force of advertising and that the Quebec legislature was reasonable in concluding that advertisers should not be allowed to capitalize on children's credulity. "[T]he particular susceptibility of young children to media manipulation, their inability to differentiate between reality and fiction and to grasp the persuasive intention behind the message, and the secondary effects of exterior influences on the family and parental authority" were the general concerns prompting this legislative response.<sup>22</sup>

The protection of children's online privacy raises much of the same concerns. Advertisers are targeting this vulnerable group in hopes of profiting from their naiveté. Thus, a similar ban on the collection of children's personal information may be the best way to protect kids from invasive online practices. Good privacy policy must be sensitive to children's developmental needs, including their need for privacy and the role that privacy plays in fostering trusting relationships with others.

### **Prohibiting commercialization of children's online play spaces**

One way in which to protect children from Internet-based media manipulation would be to introduce federal legislation that would prohibit embedded advertising in children's online games and play spaces. A template for this type of law reform can be found in ss. 248 – 249 of the Quebec *Consumer Protection Act* which prohibits advertisements targeted toward children under the age of thirteen:

Advertising for persons under 13.

248. Subject to what is provided in the regulations, no person may make use of commercial advertising directed at persons under thirteen years of age.

Criteria of intent.

249. To determine whether or not an advertisement is directed at persons under thirteen years of age, account must be taken of the context of its presentation, and in particular of

- (a) the nature and intended purpose of the goods advertised;
- (b) the manner of presenting such advertisement;
- (c) the time and place it is shown.

Presumption.

The fact that such advertisement may be contained in printed matter intended for persons thirteen years of age and over or intended both for persons under thirteen years of age and for persons thirteen years of age and over, or that it may be broadcast during air time intended for persons thirteen years of age and over or intended both for persons under thirteen years of age and for persons thirteen years of age and over does not create a presumption that it is not directed at persons under thirteen years of age.

Although having survived that early challenge, the Quebec legislative provisions were for many years thought to apply only to the broadcast sector and their enforcement

---

<sup>22</sup> *Ibid.* at 621.

was not always considered effective. In recent years, however, consumer protection movements and children's advocates in Quebec have prompted a resurgence of enforcement activity by the Consumer Protection Bureau, and rather than face charges media giants such as Nestlé, McDonald's, General Mills and others have pleaded guilty to charges for marketing schemes that were broadcast, Internet-based, or embedded in daycare healthy living campaign materials.

The Quebec legislative model could be updated and reinforced to specifically address the concerns of behavioural targeting in the Internet era. Other provinces could follow Quebec's lead by adopting either general prohibitions on marketing to children or more specialized provisions prohibiting behavioural targeting of minors and any data-mining or secondary uses of data collected from children's online play. Alternatively, federal legislation may be an option to restrict the commercialization of children's online play spaces by amending the federal *Competition Act* to make it an offence to engage in collecting information from children for the purposes of targeted marketing activities.<sup>23</sup>

### **Non-Commercial Online Play Spaces**

Another proposal to consider is the creation of online play spaces for children and youth that are not commercial in nature. As a society, we have identified a number of spaces that are protected, to some degree, from commercial interference: playgrounds, schools, libraries. As the amount of time that our children spend online increases, it may be time that we recognized this represents yet another forum where children are given the opportunity to build relationships and have fun without being unduly influenced by commercial interests.

A number of not-for-profit online resources already exist, such as Zoe & Molly Online, which is run by the Canadian Centre for Child Protection under their Cybertip.ca program. The challenge with this proposal is the possible high start-up cost and expertise necessary to develop a website children would actually like to visit. Accordingly, financial support of existing NGOs may be a feasible alternative. As the Internet becomes increasingly the media of choice for young Canadian viewers, an informed public debate should help determine the value, the cost and the means that could best protect and promote non-commercial online play spaces. The Canadian Broadcasting Corporation is a public broadcaster created by federal statute embodying the importance which Canadians have placed in public broadcasting. Should specialized legislation establish and define the public space which Canadians want to reserve to their children's safe and optimal development via the web?

---

<sup>23</sup> Valerie Steeves, "Children's Privacy: An Overview of the Federal Legislative Landscape" (July 2009).



## Law Reform to PIPEDA

The current privacy legislation in Canada, the *Personal Information Protection and Electronic Documents Act* (“PIPEDA”)<sup>24</sup> has been ineffective at dealing with the problem of protecting children’s online privacy. *PIPEDA* was introduced in the 1990’s and governs how private-sector companies can collect, use and disclose personal information. It is a consent-based model of protection that does not look at the relative maturity or age of the person offering consent, nor are the standards for ensuring the consent is informed sufficient. To put it simply, children are not differentiated from adults when considering their privacy rights.

*PIPEDA* is subject to a mandatory legislative review on a regular basis. The last review recommended legislative reform in the area of children’s privacy and Industry Canada, in response, has agreed to do this. We have yet to see meaningful legislative action on this front federally, and yet the next *PIPEDA* review is not that far off. Canadians are looking to federal and provincial parliamentarians for leadership and results as to how to keep our promises to children and to mitigate any harm to them. One suggestion as to how *PIPEDA* or substantially similar statutes at the provincial level can be amended is to shore up the consent requirements based on specific age requirements, with different levels of consent based on age categories. The following is a proposed scheme of varying consent requirements put forward by the Public Interest Advocacy Centre in a 2008 report on children’s online privacy:

1. Under thirteen: a general prohibition on the collection, use and disclosure of all personal information from children under the age of thirteen.
2. Aged 13 – 15: websites would be permitted to collect and use personal information solely in relation to that website with the explicit consent of the teen and parent and would not be permitted to further disclose their personal information
3. Aged 16 to legal maturity (18 or 19): websites would be permitted to collect personal information with the teen’s consent, and disclose the personal information of the teen only with the opt-in consent of the teen and explicit consent of a parent.
4. After attaining the age of majority: websites and corporations would no longer be permitted to retain the information gathered when the child was below the age of majority and would be required to delete the information immediately without the explicit consent of the person attaining the age of majority.<sup>25</sup>

The distinction between this suggested law reform and *COPPA* is that this law reform calls for a total prohibition on the collection, use or disclosure of the personal information of someone under the age of thirteen whereas *COPPA* simply requires parental consent. Due to the lack of success of *COPPA*, a total prohibition on the

---

<sup>24</sup> *Personal Information Protection and Electronic Documents Act* S.C. 2000, c-5.

<sup>25</sup> Public Interest Advocacy Centre, *All in the Data Family: Children’s Privacy Online* (September 2008), online: Public Interest Advocacy Centre <[http://www.piac.ca/files/children\\_final\\_small\\_fixed.pdf](http://www.piac.ca/files/children_final_small_fixed.pdf)>, p. 69-70.

collection, use or disclosure of the personal information of someone under thirteen may be a reasonable alternative.

Although the various proposed age categories will make the legislation more complicated to comply with and to administer, they may be necessary to ensure the legislation is Charter-compliant. The Canadian Charter of Rights and Freedoms guarantees the liberty and equality of all Canadians and may oblige the state to respect the decisions of children who possess the capacity and sufficient maturity to make such personal decisions about releasing personal information to website operators. The recent Supreme Court of Canada decision *A.C. v. Manitoba (Director of Child and Family Services)*<sup>26</sup> held that child protection laws must respect the decisions of mature young people provided they demonstrate they are competent to make the decision involved. The court determined that if the necessary level of maturity exists in the young person, the adolescent's views ought to be respected.

Based upon the previous *PIPEDA* review and the lack of follow-through in relation to children's online privacy, there is a clear opportunity to deliver a strong message, especially if the message is supported by interested agencies across the country. Privacy commissioners and child and youth advocates from across the country hope that by acting together with civil society we should be able to move forward this agenda appreciably.

### **Requirements for Internet Service Providers**

There can be a conflict between police officers who want access to personal information in the course of a child pornography investigation and Internet service providers ("ISPs") who require search warrants before providing customer information to investigating peace officers. ISPs are permitted to disclose personal information such as the name, address and phone number of a customer being investigated in these circumstances under current privacy legislation; however, others are hesitant to do this because of countervailing values such as privacy, free speech and freedom of association. Privacy legislation is however the shield which is used as the basis for refusing cooperation, and this has created significant confusion for officials seeking to reconcile advice from child advocates and law enforcement agencies on the one hand and privacy advocates on the other.

Currently, ISPs are not required to retain customer data, potentially frustrating police investigations into suspected child pornography users. The Canadian Coalition Against Internet Child Exploitation,<sup>27</sup> chaired by Cybertip.ca, has developed an excellent tool to assist in this. They have created a standardized letter of request for information that

---

<sup>26</sup> *A.C. v. Manitoba (Director of Child and Family Services)*, 2009 SCC 30.

<sup>27</sup> The Canadian Coalition Against Internet Child Exploitation (CCAICE) is a voluntary group of partners who work to reduce child sexual exploitation on the Internet. Chaired by Cybertip.ca, other members include the National Child Exploitation Coordination Centre, Public Safety Canada, Canadian Association of Internet Providers, AOL Canada, Bell Canada, Cogeco, TELUS, Rogers, Shaw, MTS, Yahoo! Canada, Google, and SaskTel.

can be used by police asking for access to information that sets out the reasons for the request and limits access to circumstances that involve child pornography.

Legislation has recently been tabled at the federal level that would require all ISPs to disclose a customer's name, address, IP address, and email address information upon request without court oversight. The *Technical Assistance for Law Enforcement in the 21<sup>st</sup> Century Act* (Bill C-47)<sup>28</sup> would allow authorities access to customer information without a warrant and would place new technical requirements on telecommunications companies to allow for interception by Canadian police and national security agencies. This is complemented by Bill C-46, the *Investigatory Powers for the 21<sup>st</sup> Century Act*,<sup>29</sup> which would provide police and national security agencies with new investigative powers like preservation demands and production orders to telecommunications companies and trace orders for locating a telecommunications device.

A preservation demand is a written demand made by police requiring the preservation of computer data. For the demand to be made, there must exist reasonable grounds to suspect that an offence has been or will be committed and that the computer data is in the person's possession or control and will assist in the investigation of the offence. The demand is temporary and expires after 21 days. A subsequent demand cannot be made to preserve the same data. The law ensures judicial oversight by stating that data cannot be obtained without a court order. Preservation has been the law in the U.S. since April 1996.<sup>30</sup>

A production order is a judicial order requiring a person to produce a document in their possession or control or prepare and produce a document containing data in their possession or control. To be issued, the judge must be satisfied there are reasonable grounds to believe:

- (1) an offence has or will be committed;
- (2) documents or data will offer evidence respecting the commission of the offence; and (3) the person who is subject to the order has possession or control of the documents and/or data.

This proposed legislation should be approached with caution to ensure that it balances both individual privacy and the legitimate needs of law enforcement and national security. We need to ensure that limits are imposed on the use of these new powers such that they are minimally intrusive into the privacy of individuals. The use of effective judicial oversight is one way this can be done. Canadian Privacy Commissioners issued a joint statement in St-John's Newfoundland in September of this year calling upon

---

<sup>28</sup> Bill C-47, *Technical Assistance for Law Enforcement in the 21st Century Act*, 2<sup>nd</sup> Sess., 40<sup>th</sup> Parl., 2009, online: <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4008179&Language=e&Mode=1&File=9>.

<sup>29</sup> Bill C-46, *Investigatory Powers for the 21<sup>st</sup> Century Act*, 2<sup>nd</sup> Sess., 40<sup>th</sup> Parl., 2009, online: <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=4007628&Language=e&Mode=1>.

<sup>30</sup> 18 U.S.C. 2703(f) requires an electronic communications service provider to "take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process" upon "the request of a governmental entity."

Parliament to give close scrutiny to the legislative proposals in Bills C-46 and C-47 to guard against their possible overbreadth and potential misuse.<sup>31</sup> Clear cases such as those related to child pornography and luring, where important criminal law enforcement activities can benefit from more intrusive information gathering techniques, should not be used as a foil to give law enforcement agencies carte blanche.

Any public policy debate that involves the Internet must include the issue of privacy and the legitimate privacy concerns that Canadians have. Madam Justice L'Heureux-Dubé commented in *R. v. Sharpe* on the act of striking a balance between the privacy of an individual and the protection of children from abuse:

We recognize that privacy is an important value underlying the right to be free from unreasonable search and seizure and the right to liberty. However, the privacy of those who possess child pornography is not the only interest at stake in this appeal. The privacy interests of those children...are engaged by the fact that a permanent record of their sexual exploitation is produced.<sup>32</sup>

Websites like Cybertip.ca also play a vital role in the protection of children online. Cybertip.ca is Canada's national tip line for reporting the online sexual exploitation of children. The tip line is owned and operated by the Canadian Centre for Child Protection. On average, Cybertip.ca receives more than 700 reports per month from the Canadian public. Reports to the tip line have resulted in at least 50 arrests and the removal of many children from abusive environments. Cybertip.ca also administers Cleanfeed Canada, an initiative involving the blocking of foreign-based child pornography websites containing images of prepubescent children. Since its launch in November 2006, Cleanfeed has blocked approximately 10,000 unique URLs. An appeal process exists for anyone who thinks that legal material has been blocked.

Currently, participation in blocking child pornography sites identified by Cypertip.ca is voluntary. Although all of the major ISP providers in Canada do participate, with the exception of Cogeco, every ISP in Canada should be obligated to participate in this effort. Therefore, the federal government should be encouraged to introduce legislation that would require all ISPs to block access to sites containing images of child pornography. The legislation should naturally also consider what parliamentary or judicial oversight may be required over the agency responsible for identifying such materials. However, a voluntary enforcement mechanism such as we now have where the eradication of child pornography is left as a social goal which those who, by the nature of the services they provide, unintentionally but directly facilitate its dissemination can adopt or not, is not a responsible approach. Nor is it consistent with the equal human dignity of Canadian children as guaranteed under international legal instruments.

---

<sup>31</sup> "Protecting Privacy for Canadians in the 21<sup>st</sup> Century: Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials on Bills C-46 and C-47," (September 2009), online: Privacy Commissioner of Canada, <[http://www.priv.gc.ca/media/nr-c/2009/res\\_090910\\_e.cfm](http://www.priv.gc.ca/media/nr-c/2009/res_090910_e.cfm)>.

<sup>32</sup> *Supra* at para. 189.

As noted by Signy Arnason of the Canadian Centre for Child Protection, ISPs present just one piece of a very complicated puzzle and it is important not to exclusively single out the role of ISPs when there are numerous stakeholders with a role to play in protection children from online sexual exploitation. However, these types of amendments represent a very manageable access point to advocate for change.

## **Mandatory Reporting of Child Pornography**

Another area of possible legislative amendment is to propose changes to provincial family services or equivalent legislation to require mandatory reporting of child pornography. This can be done by expanding the existing legislation that currently requires all persons to report suspicions that a child is in need of protection. Enacting such legislation would bring Canada in line with other countries, like the United States and Australia which, under federal law, require ISPs to report the discovery of child sexual abuse images. The purpose of such a law is to minimize the hurdles that law enforcement are required to jump through when attempting to access information from Internet service providers.

The enactment of *The Child and Family Services Amendment Act (Child Pornography Report) (Manitoba)* made Manitoba the first province in Canada to enact legislation which makes it mandatory for a person who encounters child pornography to report it.<sup>33</sup>

17(2) Without restricting the generality of subsection (1), a child is in need of protection where the child

...

(c) is abused or is in danger of being abused, including where the child is likely to suffer harm or injury due to child pornography;

...

### *Reporting a child in need of protection*

18(1) Subject to subsection (1.1), where a person has information that leads the person reasonably to believe that a child is or might be in need of protection as provided in section 17, the person shall forthwith report the information to an agency or to a parent or guardian of the child.

### *Reporting child pornography*

18(1.0.1) In addition to the duty to report under subsection (1), a person who reasonably believes that a representation, material or recording is, or might be, child pornography shall promptly report the information to a reporting entity.

### *Seeking out child pornography not required or authorized*

18(1.0.2) Nothing in this section requires or authorizes a person to seek out child pornography.

### *Reporting to agency only*

18(1.1) Where a person under subsection (1)

(a) does not know the identity of the parent or guardian of the child;

---

<sup>33</sup> *The Child and Family Services Act*, S.M. 1985-86, c. 8

- (b) has information that leads the person reasonably to believe that the parent or guardian
  - (i) is responsible for causing the child to be in need of protection, or
  - (ii) is unable or unwilling to provide adequate protection to the child in the circumstances; or
- (c) has information that leads the person reasonably to believe that the child is or might be suffering abuse by a parent or guardian of the child or by a person having care, custody, control or charge of the child;

subsection (1) does not apply and the person shall forthwith report the information to an agency.

*Duty to report*

18(2) Notwithstanding the provisions of any other Act, subsections (1) and (1.0.1) apply even where the person has acquired the information through the discharge of professional duties or within a confidential relationship, but nothing in this subsection abrogates any privilege that may exist because of the relationship between a solicitor and the solicitor's client.

*Protection of informant*

18.1(1) No action lies against a person for providing information in good faith and in compliance with section 18.

*Identity of informant*

18.1(2) Except as required in the course of judicial proceedings, or with the written consent of the informant, no person shall disclose

- (a) the identity of an informant under subsection 18(1) or (1.1)
  - (i) to the family of the child reported to be in need of protection, or
  - (ii) to the person who is believed to have caused the child to be in need of protection; or
- (b) the identity of an informant under subsection 18(1.0.1) to the person who possessed or accessed the representation, material or recording that is or might be child pornography.

*Retaliation against informant prohibited*

18.1(3) No person shall dismiss, suspend, demote, discipline, harass, interfere with or otherwise disadvantage an informant under section 18.

The amendment to the Manitoba *Child and Family Services Act* expanded the definition of child abuse to include child pornography. The law applies to all persons, including employers, computer technicians and Internet service providers. The *Act* states that the informant's identity is kept confidential except as required in judicial proceedings or by consent. The *Act* also protects informants who report child pornography from retaliation they could suffer. Those convicted of failing to report their reasonable suspicions of child pornography could face a hefty fine or up to two years in jail, or both.

Similar amendments requiring mandatory reporting of child pornography have been made in Ontario<sup>34</sup> as well as Nova Scotia,<sup>35</sup> although these laws are not yet in force in either province. The goals of mandatory reporting are clear: to save children from ongoing sexual abuse and to reduce the production, reproduction and distribution of child pornography. These law reform initiatives rely on the *Criminal Code of Canada's* definition of child pornography,<sup>36</sup> which moves us towards a national standard on which to measure what material constitutes child pornography. Such legislative reform reinforces the rights of children to be free from sexual exploitation and abuse.

### **Safeguarding against the distribution of prohibited Internet sites**

If Canada moves legislatively towards mandatory requirements on ISPs to retain and disclose personal information in accordance with law enforcement requests and mandatory reporting requirements on individuals who encounter child pornography, a key consideration will be to ensure that information about child pornography websites, images and videos, and child sexual abuse victims be protected from use and disclosure except in the strictest of circumstances. Lists of URLs that contain child pornographic images, repositories for child sexual abuse images and recordings, and the identity of the victims of child pornography collected in pursuit of law enforcement purposes must be carefully safeguarded. Additional private sector privacy legislative provisions may be an option to create stricter safeguards of this highly sensitive information held by non-governmental organizations that work with law enforcement and ISPs holding lists of child pornography websites and content. In a similar vein, the Federal Ombudsman for Victims of Crime has recently recommended an amendment to the *Criminal Code* to ensure that child sexual abuse material is not disclosed to defence counsel and that other opportunities for proper review of evidence be made available.<sup>37</sup>

### **Children's Privacy as a Human Right**

The Working Group has recognized the importance of taking the privacy rights and media rights guaranteed under the Convention on the Rights of the Child seriously. By using a human rights approach and recognizing the fundamental or quasi-constitutional nature of children's privacy rights, the harms outlined above and the means to address them can be placed in proper perspective. Framing the discussion in terms of privacy as a quasi-constitutional and human right compels any opposition to demonstrate why children's privacy rights do not outweigh other considerations, such as the industrial benefits sought by online applications and content developers or protecting the freedom of commercial expression.

---

<sup>34</sup> *An Act to Amend the Child and Family Services Act to Protect Ontario's Children*. Assented to December 10, 2008. [http://www.e-laws.gov.on.ca/html/source/statutes/english/2008/elaws\\_src\\_s08021\\_e.htm](http://www.e-laws.gov.on.ca/html/source/statutes/english/2008/elaws_src_s08021_e.htm)

<sup>35</sup> *Child Pornography Report Act*, S.N.S. 2008, C. 35. Assented to November 25, 2008. <http://gov.ns.ca/legislature/legc/~sol.htm>

<sup>36</sup> *Criminal Code of Canada*, R.S.C., 1985, c. C-46, s. 163.1.

<sup>37</sup> Office of the Federal Ombudsman for Victims of Crime, "Every Image, Every Child: Internet-Facilitated Child Sexual Abuse in Canada," (2009), online: Office of the Federal Ombudsman for Victims of Crime: <[http://www.victimfirst.gc.ca/pub/rep-rap/childp-pjuvenile/ovc\\_eng.pdf](http://www.victimfirst.gc.ca/pub/rep-rap/childp-pjuvenile/ovc_eng.pdf)>.

The difficulty, however, lies in defending the constitutional nature of the rights in question. On the one hand, the international legal guarantees binding on Canada are clear both in terms of the privacy rights guaranteed under Article 17 of the *International Covenant on Civil and Political Rights* and the more specific provisions relating to child privacy in Article 16 of the *Convention on the Rights of the Child*. The Supreme Court of Canada has also recognized the quasi-constitutional status of access to information and privacy statutes in Canada. However, whether this extends to PIPEDA is unclear. Despite PIPEDA's fairly straightforward purpose clause, the interpretive principles normally applicable in Canada to human rights statutes were given short shrift by the highest court when the privacy interests protected under the statute clashed with hallowed common law rights such as those governing solicitor-client privilege.<sup>38</sup> The Canadian Charter itself has no privacy guarantee and the Court has had to reverse engineer the right from the modest protection against unreasonable search and seizure in section 8 and section 7 guarantees to life, liberty and security of the person.<sup>39</sup> The privacy provisions of the *Canadian Human Rights Act* were repealed when the *Privacy Act* was adopted and the human rights value of privacy rights has been open to question since. Parliamentary privacy commissioners have often recommended constitutional change to entrench the right in the Canadian constitution, but there is very little appetite for such an undertaking.

What then can be done to require Canadians and others subject to our jurisdiction to take children's privacy rights seriously?

One idea canvassed in Fredericton which may have some traction and is a possible area for consensus building is to focus narrowly on the task at hand. Constitutional amendments in Canada cannot be sought by the faint of heart, a great deal of stamina and political will has to be mustered in order to support change of that nature. The consensus can be built however in stages looking first to the areas of broadest consensus. The need to protect children's privacy in the 21<sup>st</sup> century is no doubt a topic upon which the broadest consensus of opinion in Canada may be found. Short of constitutional change of the kind described above, the most practical way forward to build towards revised foundational norms in Canada is to perfect the area of human rights laws which our courts have qualified as quasi-constitutional.

In June of this year, a private member's bill was tabled in Parliament calling for the creation of a Children's Commissioner for Canada.<sup>40</sup> The UN Committee on the Rights of the Child has been promoting the creation of such national institutions as the best means possible of entrenching the guarantees of the Convention within domestic and national laws. This initiative would be consistent with Article 4 of the CRC, which

---

<sup>38</sup> *Privacy Commissioner of Canada v. Blood Tribe* [2008] 2 S.C.R. 574

<sup>39</sup> *R. v. Dyment*, [1988] 2 S.C.R. 417 at para. 17. Laforest J.'s oft-quoted passage reads as follows: "Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for the public order."

<sup>40</sup> Marc Garneau. A national Children's Commissioner for Canada. June 11, 2009: <http://www.marccgarneau.ca/en/latestnews.aspx?id=823>.



requires that a signatory do all that it can to ensure that it is compliant with the Convention. A recent Senate study found that despite Canada's ratification of the CRC, it has been "effectively marginalized when it comes to its direct impact on children's lives."<sup>41</sup> The Committee on the Rights of the Child has specifically called for such a position to be created in Canada.<sup>42</sup> Canada could show leadership by creating a Children's Commissioner for Canada and adopting by reference as part of the Commissioner's constituent statute the rights set out under the Convention including the privacy rights guarantees set out in Article 16 of the Convention. The Commissioner could also be given specific enforcement powers with respect to these provisions given the prevalence of privacy concerns to Canadian children today.

Establishing a position such as this in Canada is effectively the difference between simply handling complaints reactively and proactively advocating for the rights of children and ensuring compliance with CRC. A national children's commissioner with broad human rights powers would be able to ensure that advertisers and commercial game developers be held accountable through a domestic human rights remedy.

Alternatively, provincial legislatures could consider expanding the scope of existing human rights legislation to encompass not only non-discrimination rights but other fundamental rights such as privacy. Provincial legislatures might also consider giving information and privacy commissioners the powers necessary to enforce broad human rights remedies in relation to privacy violations. Children's privacy rights are particularly unlikely to be enforceable before civil courts: the age of the victims, their means, their capacity, the nature of the harm suffered and the value which society and sometimes that which youth themselves place upon it all conspire against this. However, with the advent of social networking it is particularly likely that the privacy interests of adolescents will be at increased risk due to sexting, cyber-bullying or defamatory messages. The cost in terms of resilience, self-esteem, quality of life and productivity may have far-reaching societal consequences if these concerns are not adequately addressed. Ensuring that accessible, enforceable and timely remedies exist to guard against this type of conduct would be a responsible legislative safeguard. Clearly educational and promotional campaigns to these same ends must continue, but stronger laws are need now to reinforce the view that children's rights are taken seriously.

## **Conclusion**

The time is ripe for action to protect children's online privacy. November 20<sup>th</sup>, 2009 marks the 20<sup>th</sup> anniversary of the Convention on the Rights of the Child and would be

---

<sup>41</sup> Canada, Standing Senate Committee on Human Rights. "Children: The Silenced Citizens: Effective Implementation of Canada's International Obligations with Respect to the Rights of Children" (2007), online: Standing Committee on Human Rights <http://www.parl.gc.ca/39/1/parlbus/commbus/senate/com-e/huma-e/rep-e/rep10apr07-e.htm>

<sup>42</sup> Committee on the Rights of the Child. "The Role of Independent National Human Rights Institutions in the Protection and Promotion of the Rights of the Child." 15/11/2002: [http://www.unhchr.ch/tbs/doc.nsf/\(symbol\)/CRC.GC.2002.2.En?OpenDocument](http://www.unhchr.ch/tbs/doc.nsf/(symbol)/CRC.GC.2002.2.En?OpenDocument)

the ideal time for Canadian law-makers to take the lead in promoting law reform initiatives to strengthen children's privacy at home. The exploitation of children's online privacy is an issue that cannot be ignored; action by way of legislative reform is needed.

This paper has explored some of the possible amendments that can be made to existing legislative instruments to better protect the online privacy of children. Its objective is to stimulate discussion among interested legislative oversight bodies and among Canadians in general in accordance with the view that many voices acting in unison will be more effective in promoting the required changes.

The ongoing cycle of *PIPEDA* reviews or of substantially similar legislation at the provincial level provides an opportunity to exert influence to ensure the legislation is amended in a manner that will make it more effective in protecting children's online privacy. *PIPEDA* could be amended to include clear consent rules for the collection, use and disclosure of children's privacy information. The development of non-commercialized online play spaces should be encouraged. Laws are needed either at the provincial or federal level to prohibit both embedded advertising in websites geared toward children and marketing efforts which are targeted to children. Quebec's consumer protection laws hold some promise in this respect, but could be updated in the information age and copied in other Canadian jurisdictions.

We also have an opportunity to help dedicated law enforcement professionals more effectively find child pornography offenders by encouraging the enactment of legislative instruments that would require ISPs to assist in child pornography law enforcement. Finally, we have the opportunity to identify more of these offenders by introducing legislation requiring mandatory reporting of encounters with child pornography. Striking the appropriate balance between the privacy rights of ISP clients and the privacy interests of children compromised by pornographers will require careful consideration, but joint advisory efforts by privacy commissioners and child and youth advocates are most likely to provide a solid basis for consensus solutions in this respect.

Aside from legislative change, we have to ensure that the laws we currently have in place to protect children's privacy are properly adhered to. For example, the Privacy Commissioner of Canada recently found the social networking site Facebook to be in violation of Canadian privacy laws.<sup>43</sup> The complaint against Facebook related to the company's unnecessary and non-consensual collection and use of personal information. The Commissioner found that the company did not alert users about how that information was being used and did not adequately destroy user data after accounts were closed. Moving forward, the focus must be on working with the tools in place to protect children's online privacy and simultaneously seeking improvements to fill the gaps that will inevitably present themselves as technology and society continue to evolve.

---

<sup>43</sup> Information Commissioner of Canada, *PIPEDA Case Summary #2009-008*, online: <[http://www.priv.gc.ca/cf-dc/2009/2009\\_008\\_0716\\_e.cfm](http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.cfm)> .

Given the domestic prevalence of the Internet in children and young people's lives, parents should not be solely charged with the responsibility to regulate children's online privacy. Legislative amendments, along with strong public awareness and educational campaigns, will better protect their online privacy and make the Internet a safer place for children.

## Appendix I - Summary of Legislative Reform Proposals

Reform Proposal	Mechanism(s)	Existing models
1. Limit/prohibit online collection of children's personal identifying and non-identifying information through commercial websites	<ul style="list-style-type: none"> <li>• New federal legislation specific to children's online privacy</li> <li>• Amendments to existing federal PIPEDA</li> <li>• Provincial amendments to substantially similar private sector legislation</li> </ul>	<i>Children's Online Privacy Protection Act (U.S.)</i>
2. Limit/prohibit advertising directed at children under the age of 13	<ul style="list-style-type: none"> <li>• Federal <i>Competition Act</i> amendments</li> <li>• provincial consumer protection legislation</li> </ul>	<i>Consumer Protection Act (Quebec)</i>
3. Prohibit embedded advertising in children's online game and play spaces	<ul style="list-style-type: none"> <li>• Federal <i>Competition Act</i> amendments</li> <li>• provincial consumer protection legislation</li> </ul>	<i>Consumer Protection Act (Quebec)</i>
4. Require ISPs to retain customer data to assist with law enforcement activities	Federal legislation as ISPs fall under federal jurisdiction as telecommunications entities	Proposed <i>Technical Assistance for Law Enforcement in the 21<sup>st</sup> Century Act (Bill C-47)</i>
5. Require ISPs to disclose customer personal information for the purpose of law enforcement activities	Federal legislation as ISPs fall under federal jurisdiction as telecommunications entities	Proposed <i>Investigatory Powers for the 21<sup>st</sup> Century Act (Bill C-46)</i>

6. Require ISPs to block access to sites containing images of child pornography	Federal legislation as ISPs fall under federal jurisdiction as telecommunications entities	Cybertip.ca
7. Mandatory reporting of child pornography for all persons (including ISPs)	Amendments to provincial child and family services legislation or separate provincial legislation	Manitoba <i>Child and Family Services Act</i> , s. 18 (in force as of April 2009) Ontario <i>Child and Family Services Act</i> amendment (not yet in force) Nova Scotia <i>Child Pornography Report Act</i> (not yet in force)
8. Prevent child sexual abuse materials from being disclosed to defence counsel during criminal proceedings	Amendment to <i>Criminal Code of Canada</i>	

<p>9. Enshrine children’s right to privacy</p>	<ul style="list-style-type: none"> <li>• Constitutional amendment to enshrine privacy rights in Charter</li> <li>• A Children’s Privacy Rights Charter</li> <li>• Children’s Commissioner’s for Canada with power to enforce Convention rights including privacy</li> <li>• Provincial amendments to human rights codes to include privacy rights</li> <li>• Provincial Commissioners given human rights tribunal remedial powers to protect privacy</li> </ul>	
--	---	--

**Statutory Offices participating in the Working Group:**

- New Brunswick Child and Youth Advocate
- Privacy Commissioner of Canada
- British Columbia Representative for Children and Youth
- Alberta Child and Youth Advocate
- Commission d'accès à l'information du Québec
- Nova Scotia Ombudsman's Child and Youth Services Unit
- Newfoundland and Labrador Information and Privacy Commissioner's Office