International Municipal Lawyers Association
74th Annual Conference, Miami, FL

Work Session XII: Libraries —
"Quiet, Please!" Doesn't Apply!
Legal Issues Confronting Public
Libraries in a Digital Age

Libraries Have Rules about that, eh!

Mary Ellen Bench
City Solicitor
City of Mississauga

©2009 International Municipal Lawyers Association. This is an informational and educational report distributed by the International Municipal Lawyers Association during its 74th Annual Conference, held October 17-21, 2009 in Miami. FL. IMLA assumes no responsibility for the policies or positions presented in the report or for the presentation of its contents.

Libraries Have Rules about that, eh!

Prepared by: Mary Ellen Bench, City Solicitor
City of Mississauga

> "All persons in Canada have the fundamental right, as embodied in the nation's *Bill of Right*s and the *Canadian Charter of Rights and Freedoms*, to have access to all expressions of knowledge, creativity and intellectual activity, and to express their thoughts publicly. This right to intellectual freedom, under the law, is essential to the health and development of Canadian society."[1]

The above statement is taken from the position statement on intellectual freedom of the Canadian Library Association. It recognizes the responsibility of libraries to ensure that the public is able to access the library's materials and information without fear of censorship, and in a safe environment. The growing use of computers and internet use within libraries and internet use pose new questions regarding how libraries will respect intellectual freedom and an individual's right to access information without violating the rights of other patrons from being exposed to objectionable information.

Provincial legislation provides that municipalities may enact by-laws establishing public libraries and appointing library boards to manage the operations of the libraries. In the Province of Ontario, the *Public Libraries Act*[2] provides that public library boards are corporations without share capital under Part III of the *Corporations Act*[3]. Board members are appointed by municipal councils and have the same fiduciary responsibilities as directors of other non-share corporations. Public library boards are charged with providing efficient public library services, in French where appropriate, as well as operating such additional services as considered necessary. Staffing and personnel matters, the acquisition of land and the construction or purchase of buildings require the approval of municipal councils. The board is responsible for appointing the public library Chief Executive Officer and individual employees, within the budget provided to it by the municipality. Public libraries in Canada primarily rely on local governments for funding. In discharging their duties, library boards are held to a standard of reasonableness.

Legislation provides that public libraries must provide free admission and free use of materials on site. Charges can however be applied for non-residents and for extra services, such as internet access. Although there is no express legal

---

1 Canadian Library Association, Position Statement on Intellectual Freedom, 1985.

2 *Public Libraries Act*, R.S.O. 1990, CHAPTER P.44.

3 *Corporations Act*, R.S.O. 1990, CHAPTER C.38.

obligation to do so, libraries are committed to ensuring that principles adopted by the Canadian Library Association and its Provincial counterparts regarding intellectual freedom are met, and ensure collections contain a wide variety of materials, reflective of the diverse interests of the community that will be using each branch, as well as appropriate facilities in which to access them. These principles extend to the access of materials and information over the internet.

While the public has a statutory right to access public libraries, libraries have authority to put in place reasonable policies necessary to regulate conduct. The extent to which libraries have formalized such policies varies considerably. The chart attached to this paper as Appendix 1 illustrates the types of policies put in place in some of Canada's largest cities and some border municipalities as well.

Internet Use in Public Libraries

Public internet use is widespread in libraries and issues arise concerning the authority of libraries to regulate internet use. The potential for criminal liability resulting from internet usage at public libraries is a serious concern. The *Criminal Code of Canada* contains restrictions on the content of communications, including internet communications with respect to obscene material, child pornography, hate propaganda and sedition. The internet is unregulated and there is no foolproof way for libraries to protect themselves from the potential for criminal liability. There are several "due diligence" initiatives that can be put in place to protect libraries from liability. These include appropriate internet policies, complaints procedures, staff training to recognize illegal or unacceptable internet usage, and the strategic use of filters to restrict access to objectionable materials.

Internet Use Policy

An internet use policy will establish the terms and conditions by which patrons are allowed to use computers in public libraries. Internet policies will often contain administrative procedures regarding how to log on, limitations on time and printing, and may ask users to take into account others in the vicinity when accessing internet sites.

Public libraries, unlike schools, are not generally required to act *in loco parentis* regarding children and minors who use their facilities. Internet use policy elements that would create an effective defence of due diligence include the following:

- individuals are subject to government legislation including the *Criminal Code*, and that the internet must not be used for illegal purposes;
- use for illegal purposes may result in prosecution;
- computers are located in public areas and patrons must not display material

which "in the opinion of any library staff" is unlawful, obscene, abusive or otherwise objectionable;

- identify whether the library network is open and if librarians can monitor materials viewed through the network;
- remind parents that it is their responsibility to monitor the activities of minors and that they are responsible for what minors might access;
- advise that an individual patron's access to the network can be modified or discontinued without notice and without liability at any time;
- prohibit users from installing or running programs on any public computer;
- advise that the library is not responsible for any copyright infringements;
- advise that the library cannot guarantee internet security and confidentiality and that internet transactions are at the patron's own risk, especially discourage against personal information, online banking or credit card transactions;
- advise that library staff have the right to monitor internet usage;
- establish an acceptable use policy reminding patrons not to disturb or interfere with the privacy rights of others;
- advise of the consequences for breach of the internet use policy. These consequences may include suspension of library privileges, exclusion from the library and/or prosecution.

Internet Filters

Most software filters block words, phrases, subjects and sites. The use of filters may block illegal or objectionable material however they cannot be relied upon to fully address the problem. The use of filters also raises a serious concern. Software filters cannot discriminate when blocking words or phrases, between unsuitable sites and sites that are educational and appropriate. Good material will always be blocked out in addition to objectionable material. Modifying software to address filtering problems will create new problems for public libraries. Legal advice obtained by the Vancouver Public Library advised that as soon as software is modified the party doing so has taken on liability as an editor of the content rather than just a conduit.[4]

The use of filters also raises a question concerning a potential violation of Section 2(b) of the *Charter of Rights and Freedoms* guarantee respecting freedom of expression. Section 1 of the *Charter* guarantees that the rights and freedoms, including freedom of expression, are subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society. Filters raise a question about the reasonableness of this limitation on an individual's right to access information.

4 "To Filter or Not to Filter? Burlington Library Seeks Legal Opinion", Derek Weiler, Quill & Quire, March, 1999.

Many library boards have struggled to assess the extent to which the use of internet filters constitutes a reasonable limit on freedom of expression. The solution adopted by many libraries has been to place internet filters strategically, using them on computer terminals in children's areas in the library while placing few or no restrictions on internet access in portions of the library generally used by adults only. If a library only has one internet workstation, the consensus seems to be that access should not be filtered.

Facebook and Social Media Policies

The growing popularity of social networking online in general has convinced many public libraries to use it to reach the community. The Canadian Association of Public Libraries as well as several municipal public libraries all have Facebook pages. Four years ago a new social networking site that caters to book lovers and libraries was developed called "Library Thing". Today it boasts several million members including libraries and individuals, and is accessible in 8 languages. It allows members to review and comment on books, have private watchlists viewable only by their friends. It advises that its collection includes materials from sources such as the Library of Congress, the Canadian National Library, Yale University and the British Library. Facebook pages established by libraries tend to have separate sites for staff and former staff to communicate, for library patrons to communicate with each other and staff, and for youth to communicate with library staff or each other.

At this time it is difficult to tell what the implications of using social networking tools will be for libraries. Again, due diligence should be exercised when considering establishing social media sites for libraries. A social media policy should be established, which in many respects would be similar to an internet access policy. The ability of individuals to post opinions on a site operated by the library does require supervision and some additional rules regarding useage. A social media policy should include provisions respecting the following:

- clearly stating that the library does not act in the place of or in the absence of a parent when minors access this resources;
- the general rules respecting use of the library apply to social media sites established by the library;
- the use of social media for any purpose which would contravene any legislation or government regulation, or which might create civil liability by the user or the library to any person, is strictly prohibited. This would include *Criminal Code* prohibitions against child pornography, obscenity, hate literature, sedition and would also include materials regarding illicit drug use. In respect of civil liability, this would include the law of libel and slander;

- all social media sites affiliated with the library will be monitored and screened by library employees. Postings which contain any of the following will be removed and the offender will be barred from posting any subsequent messages to library social media sites: postings shall not contain obscene obscene or racist content; personal attacks, insults or threatening language; potentially libellous statements; plagiarized material; private, personal information published without consent; comments totally unrelated to the content of the forum; hyperlinks to material that is not directly related to the discussion; or commercial promotions or spam; organized political messaging;
- some sites also contain a requirement that users must indemnify the public library including its officers and employees from any judgments, damages, liabilities or costs incurred or related out of the posting;
- finally, users should be requested to agree to these terms and their agreement should be noted before they are able to access the site.

Regardless of the policies in place, it is important to note that social network sites cannot fully protect the privacy of users. In 2008 the Canadian Internet Policy and Public Interest Clinic (CIPPIC), based at the University of Ottawa, Faculty of Law, asked the Privacy Commissioner of Canada to investigate 22 alleged violations of Canadian privacy law by Facebook. Included in the allegations was that Facebook members were not adequately advised that their personal information could be disclosed to third parties for advertising and other profit-making activities; that Facebook did not obtain permission from users to access their personal information and that the security settings were inadequate. On July 16, 2009, the Assistant Privacy Commissioner of Canada, Elizabeth Denham released her report titled "Report of Findings into the Complaint Filed by the Canadian Internet Policy and Public Interest Clinic (CIPPIC) Against Facebook Inc. Under the Personal Information Protection and Electronic Documents Act". On the issues of default privacy settings and advertising, the Assistant Commissioner found that Facebook was in contravention of the Act but that corrective measures had been taken by Facebook to respond to her recommendations. On issues respecting deception and misrepresentation including Facebook Mobile the Commission found that the allegations were not supported by the evidence. The Commission found contraventions of the legislation that had not been adequately addressed in respect of the subjects of third-party applications, account deactivation and deletion, accounts of deceased users and non-users' personal information. The investigation focussed only on users in Canada over 18 years of age. The concern was the extent to which the public is leaving their "digital footprints" everywhere and Facebook was selected by the CIPPIC because of the extent to which it was used by its members. The report concludes by providing Facebook with a 30 day period to comply, failing which the Commissioner will consider the appropriate action to be taken. To date, this matter remains unresolved.

Technology and Privacy Rights

Public libraries are subject to provincial legislation respecting freedom of information and protection of privacy. Libraries must therefore take reasonable steps to ensure that personal information about patrons which is in their custody or under their control is secure against unauthorized collection, use, access, disclosure or disposal regardless of the form of that information. In terms of computer or internet usage, libraries collect information through policies that require patrons to identify themselves online by library card number or to sign in a register or book to secure a timeslot to use the computer. Libraries also collect information on the computer hard drive about the sites and useage of each computer by patrons who have been authorized to use it. Patrons who bring their own laptop or other wireless device to the library will be subject to all library use policies as well.

In public libraries, privacy safeguards include measures to ensure that employees and volunteers of the library only access the personal information of patrons to the extent necessary or required to perform their job duties. It is important that they receive training on policies respecting freedom of information and protection of privacy, and confidentiality agreements may even be required. Some libraries also include policies respecting the placement of terminals and screens to ensure that unauthorized persons cannot view the information being called up by patrons on the screen.

While library patrons have the right to confidentiality and privacy when using electronic information networks, policies must provide that where complaints are received from patrons that a user is accessing legally prohibited material, library staff may intervene.

Canadian courts have had occasion to consider whether e-mails intercepted by an internet service provider are private or whether they can be used as evidence in a *Criminal Code* matter.[5] In this case the defendant was charged with possession of child pornography based on evidence obtained from his e-mail when his internet service provider was repairing his computer. The internet service provider informed the police who obtained a search warrant and seized Weir's computer and disks. The Alberta Court of Queen's Bench determined that while the defence suggested internet e-mail carried a reasonable expectation of privacy, there was no Canadian case law to support this, and the very nature of the technology made it vulnerable to third party access. The conviction was upheld.

Surveillance

Library surveillance through Closed Circuit TV (CCTV) or other audio,

5 *R. v. Weir* [1998] 8 A.J. No. 155, 59 Alta. L.R. (3d) 319.

visual or electronic surveillance are only authorized for use as a last resort. Libraries should be prepared to show that other means of monitoring the activities of patrons that are substantially less invasive are not effective, before installing such systems. When surveillance systems are installed, efforts should be made to ensure that they are designed to achieve their goals with the least privacy invasion possible. One way of doing this is to place signage ensuring that patrons are aware of the surveillance and through strategic placement of surveillance equipment.

WiFi

There is a growing trend to provide WiFi access within public libraries. Wireless connections are inherently unsecured and accessible by third parties, thus the reason for appropriate policies to be in place and disclaimers to protect libraries from liability. Most of these policies stipulate that patrons should be careful about security since WiFi is an open forum, and wireless transmissions are capable of being intercepted by others. Policies on acceptable use of wireless connections also reiterate library policies prohibiting patrons from using them to seek information that is illegal, actionable or for criminal purposes. Essentially the same rules that apply to internet use in libraries should apply to use of the WiFi network within public libraries. Compliance is often achieved by requiring users to click on "I agree" or "Ok" in order to be able to successfully log onto the wireless network.

There is very little Canadian case law on the issue of electronic communications and no reported cases could be found on the issue of internet or WiFi usage with public libraries in Canada. In terms of the general policies outlined above, a case of interest is *R. v. Cheung*[6]. This is a decision of the British Columbia Supreme Court where the police intercepted cellphone communications in order to obtain evidence of criminal activity. The defendant argued that the interception of the cellular telephone conversations was not authorized in accordance with the provisions of Part VI of the *Criminal Code*, "Invasion of Privacy". The *Criminal Code* only permits the interception of private communications where there is proper authorization. In that case the court held that the communications made on a cellular telephone were private communications within the meaning of the *Criminal Code* and while it was possible to eavesdrop on cellular calls by using a scanner, it would have been practically impossible for the police to intercept the calls of particular individuals in the fashion that they did. The court held that the test to be applied in interpreting whether the communication was private was the reasonable expectation of a user of a cellular telephone. On that basis the court determined that cellular telephone calls are private communications and can only be intercepted by the police with proper authorization. It may be that a court would take the same approach in respect of the interception of communications from a WiFi user.

6 *R. v. Cheung* [1995] B.C.J. No. 1751, 100 C.C.C. (3d) 441.

Children as Users of the Library

While there is no legal requirement for public libraries to treat children any differently than any other group of library patrons, as previously noted, many library policies relating to internet usage and filtering, and even the location of library materials in a separate children's area, support an acknowledgment that libraries must be aware of children using their facilities without treading upon the rights to intellectual freedom espoused by the Canadian Library Association. Without accepting the responsibility of monitoring what children access, appropriate policies can protect the rights of the diversity of users who come into the library. While there does not appear to be any Canadian case law that confirms this position, it has been considered several times in the United States. The California courts have had cause to consider it in the case of Kathleen R. et al. v. City of Livermore[7]. The facts of this case are that Kathleen R.'s 12-year old son used a library computer to download sexually explicit photographs from the internet onto a floppy disk that he had brought to the library. He then copied the material and provided it to other minors. The library had an internet access policy that provided in part that it supported the idea of free and equal access by all to the entire range of library resources, and that such rights extended to minors. The policy stressed in multiple locations that it does not monitor or supervise internet access and provided that it was the responsibility of parents to determine what was appropriate and to supervise their children's use of the internet consistent with their values. Kathleen R. alleged that the library "knowingly and intentionally" allowed its computers to be used to display obscene and pornographic images where children could view them and sought damages. The Court of Appeal recognized that a public library is in a "damned if you do, damned if you don't" situation in deciding whether to restrict access to the internet from its computers to prevent harm to minors. The court cited other decisions where courts upheld claims against libraries who used filtering software on the grounds that this violated the First Amendment. The Court of Appeal upheld the decision of the lower court and found that there was no constitutional duty on government to protect children from harmful material on the internet.

Joint Use Libraries

In today's economic climate, schools/public library amalgamations are becoming popular. Often public libraries and community centres are combined with schools under joint use agreements. While there are certainly funding benefits to this model and the synergies can result in greater library, there are also a number of drawbacks. School libraries are governed by different legislation with different goals and objectives. The primary responsibility of the school library is to the educational program of the school and its collection is an integral part of the instructional system.

---

7 *Kathleen R. et al. v. City of Livermore* 87 Cal. App. 4th 685; 104 Cal. Rptr. 2(d) 772; 2001 Cal. App. LEXIS 158; 2001 Cal. Daily O.p. Service 1898; 2001 Daily Journal DAR 2383.

Censorship issues respecting materials appropriate for adults is a key issue. The censorship concern is greatest when the school in question has a religious affiliation, as has been raised given the popularity of this arrangement involving Catholic school boards.

The Recommendations to the Minister of Saskatchewan Municipal Government from the Saskatchewan Municipal Trustees' Association as Proposed by the Committee on School/Public Library Cooperation[8] references a quote from a paper on joint use libraries that sets out the problem in a nutshell:

> "Unfortunately, many of the decisions to create joint use libraries and the operational agreements that accompany them are being made at high levels of administration with little or no input from experienced library professionals who will ultimately be responsible for running these potential ulcer mills. The opportunity for excellence in terms of library services and facilities can be and often is equal to the potential for causing a great deal of frustration and dissatisfaction for the staff."[9]

There are many administrative concerns with joint use school/public library facilities including, providing appropriate security for schoolchildren from adults, especially during school hours; providing for access when schools are closed; determining the protocols and procedures for adding materials to the library collection and whether such procedures meet the requirements of legislation applicable to both school and public libraries; providing for a system by which public libraries maintain their right to circulate their collection from branch to branch; jurisdiction, authority and supervisory issues when staff from two library services are merged; to name a few.

Bill 128, Christopher's Statute Law Amendment Act (Sex Offender Registry and Electronic Sexual Material), 2008

Bill 128 is a Private Member's Bill that received first reading in the Ontario Legislature in November 2008. A copy of the Bill is attached as Appendix 2. This Bill seeks to amend both the *Education Act* and the *Public Libraries Act* in Ontario to make mandatory measures for all school and public library computers to which a minor could have access to block access on the internet to any material that is sexually explicit or constitutes child pornography as defined in the *Criminal Code*; to block access to any form of electronic communication that could expose a minor to

8 The Recommendations to the Minister of Saskatchewan Municipal Government from the Saskatchewan Municipal Trustees' Association as Proposed by the Committee on School/Public Library Cooperation, April 9, 1995, Saskatchewan Library Trustees' Association, Saskatoon, Saskatchewan.

9 Ibid, p. 8, from I.S. "Bud" Call B.C. "Joint Use Libraries: Just How Good are They?", C&RL News (Nov. 1993), page 551-552.

obscene, sexually explicit or (child) pornographic material as defined in the *Criminal Code*. In addition, policies for authorized access must be in place under the proposed bill, to monitor electronic access by minors.

Bill 128 causes concern for a number of reasons. First, it is very doubtful that filtering software currently available on the market can actually do what the Bill requires. There is no software available that can successfully block access to inappropriate material. Attempts by public libraries to modify software would attract potential liability as an editor of material. Setting aside any *Charter of Rights and Freedoms* concerns about restricting Section 2 rights without just cause, there is also a concern that library staff may not be able to always identify such illegal material, which could also attract liability. It appears as well that the drafter of the proposed legislation fails to recognize that most libraries already have in place comprehensive policies dealing with internet usage and the usage of electronic devices within their premises, to protect against patrons accessing illegal materials.

Use of Library Computers and Terrorism: The "Toronto 18"

In December 2005, a group that became known as the "Toronto 18" held a training camp in Washago, Ontario for the purpose of training potential recruits for a terrorist group. Fourteen adults and four youth were charged in a massive police sweep during the summer of 2006. Many of the details remain subject to a publication ban. At the first trial held in 2008, prosecutors made public that some of the group's members were planning to bomb sites such as the Toronto Stock Exchange, the RCMP headquarters in Ottawa, the Pickering Nuclear Power Plant and the Toronto offices of Canada's spy agency, CSIS, which is located next to the CN Tower. This was also one of the first trials held under Canada's *Anti-Terrorism Act*, a controversial bill passed shortly after the September 11, 2001 attacks. The Act gives police far-reaching powers to disable suspected terrorist threats, including preventative arrests and the right to detain suspected terrorists for up to three days.

One of those charged, Saad Khalid, a 23 year-old Mississauga resident was charged with knowingly participating in a terrorist group, receiving training for the purpose of enhancing the ability of a terrorist group and doing things with "intent to cause an explosion of an explosive substance that was likely to cause serious bodily harm or death". He pleaded guilty to the last charge respecting the explosives.

While many of the facts surrounding the charges against the Toronto 18 still remain the subject of a publication ban because several of the accused have yet to be tried, certain facts became public in a Statement of Uncontested Facts filed in court at the time of Khalid's guilty plea. Among those facts was an admission that Khalid visited a Mississauga library to research the fertilizer ammonium nitrate and other matters related to bomb-making. The Statement of Uncontested Facts contains the following:

"March 22, 2005

5. At 9:35 am, _____was observed entering Meadowvale Library and using a computer. The computer was later seized and the hard drive was analyzed. Amongst the searches conducted by _____ were "ammonium nitrate in agriculture", "nitric acid", "rocket fuel", "fuel tablets", "buy nitric acid".
6. Later that night, at approximately 7:00 pm, _____ drove to a school in Mississauga where he picked up Saad Khalid. They drove together _____ car to Hamilton, Ontario. At approximately 8:00 pm _____ and Khalid went into a house in Hamilton. Shortly thereafter they emerged from the house accompanied _____. The three men walked together into the campus of McMaster University. From approximately 8:22 to 9:22 pm _____ Khalid and _____ sat talking together. A video was taken of this meeting _____ and Khalid then left _____ Khalid were together until _____ dropped off Khalid in Mississauga at approximately 10:40 pm.

…

March 30, 2006

10. _____ was observed entering the Meadowvale Public Library and working with a soldering iron, spools of wire and batteries. _____ was also observed using a computer. The computer was later seized and the hard drive was analyzed. It was discovered that _____ had used the computer to order business cards bearing the name "Student Farmers".
11. Later that same day, at approximately 3:04 pm, _____ played basketball at Meadowvale Community Centre. They finished playing basketball and left the area in separate cars.
12. At 3:47 pm, _____ was observed to enter Bali Electronics. A store employee was overheard telling _____ "the switch will open when activated by light". The store employee later explained to the police that his conversation with _____ had been about a photocell device.

April 3, 2006

13. At approximately 2:10 pm _____ was observed to enter the Meadowvale Public Library and use a computer. The computer was later seized and the hard drive analyzed.

Amongst the searches conducted by _____ were: "fertilizer", "explosive", "ways of getting ammonium nitrate".

April 7, 2006

..

15. Later that evening (and into the early hours of April 8th) Shaher Elsohemy, the second police agent ("the agent"), met with _____. Their meeting commenced inside the gas bar and later continued at a nearby restaurant. They discussed the following:

- _____ laid out a terrorist plot to bomb three locations in the Greater Toronto Area. The plot involved the rental of three U-Haul vans, which they would pack with explosives. The vans were to be parked at three locations and the explosives were to be triggered remotely. The locations were: the Toronto Stock Exchange ("TSE"), the CSIS headquarters on Front Street in Toronto, and an unspecified military base.
- _____ said that he plans to do the attacks in mid November 2006. He said he wants to conduct the attacks around 9:00 a.m. and be on a plane by 10:00 or 10:30.
- _____ said that the detonator is ready, that he has tested it and it works. He said he made the detonator with his own hands. He said it is very sophisticated and can be activated even from another city.
- _____ said he considered building the bombs out of either RDX or a combination of ammonium nitrate and nitric acid. _____ described from memory the explosive velocity of both RDX explosives and ammonium nitrate explosives. He said RDX is more powerful, however it is difficult to obtain. Therefore he ruled it out and decided to use ammonium nitrate.
- _____ laid out two plans for procuring the ammonium nitrate: "Plan A" involved securing a contact who could supply chemicals in large quantities. Failing that, "Plan B" involved _____ and two unnamed friends purchasing fertilizer, bleach and household items from which they would make the bombs. _____ said that if the three of them purchase these items in small quantities they will not raise any suspicion.
- _____ took out a piece of paper and wrote down the chemicals that he required to produce these bombs. The paper had the following handwritten notation on it:
    (1) Nitric Acid (98% - 95 – 90) (2 gallons)
    (2) Ammonium Nitrate + (1.5 tons)

- _____ handed this paper to the agent (who later turned it over to the authorities). _____ asked the agent if he could help procure these chemicals. The agent responded that he might be able to help.
- _____ said he plans to rent the three U-Haul vans, using fake identification.
- _____ wanted to have the agent and _____ find a house to rent, so that _____ two friends can live in the place, store the materials and build the bombs.
- _____ said that this was the first time he was telling anybody about the whole plan, and indicated that these two friends don't know anything yet."

…

April 26, 2006

25. On April 26th the agent met _____ in the Café de Khan in Mississauga. They discussed the following:

- _____ asked the agent to provide plane tickets for _____ and his family to travel to Saudi Arabia departing on August 1st for one month. _____ explained that when he returned, he would disappear for five days to set up the devices and the detonation would take place in early September. _____ said that he had the detonator in his car and wanted to show it to the agent and _____. The agent told him to wait until tonight.
- _____ said he has $20,000 in cash. He reiterated that he wants the agent to rent a house in which they can assemble the devices and store the chemicals.
- _____ said he would purchase four USB computer memory sticks ("memory sticks") which will be used _____ to communicate with the other two "co-conspirators" so that they won't have to use the phone or e-mail. The devices will store instructions and will be passed back and forth.
- _____ said he will give each of the two co-conspirators $5,000 to purchase quantities of ammonium nitrate.
- _____ said if the agent were to provide low-grade ammonium nitrate, he knows a way to purify it using coffee. He asked the agent to supply the highest purity of nitric acid available.

It becomes very clear from the Statement of Uncontested Facts that the accused relied heavily on information obtained over the internet. Computers were

seized from the library and from a variety of other locations including their homes, and the group transferred this data between members using USB computer memory sticks.

The seizure of information from the Mississauga Public Library branch was not contested. The question this raises for municipal lawyers is what do you do when the police arrive wanting access to library computers? If the police arrive with a properly executed warrant, staff are obligated to turn over the documents, records or equipment referred to in the warrant. When police do not have a warrant, for library staff to breach the privacy rights of its patrons it is incumbent upon staff to ensure some system is in place to validate the reasonableness of employees turning over the requested material. In the City of Mississauga we have developed a form which records the documentation or equipment requested for law enforcement purposes, the name of the law enforcement agency (it could be local, provincial or a federal police force) and identifies in very general terms the reasons for the release. There are three reasons in which the City will authorize staff (including library staff) to release materials to the police without a warrant:

(1) for law enforcement purposes; or
(2) the health or safety of an individual is at risk; or
(3) in compassionate circumstances to facilitate contact with next of kin or a friend.

A copy of the form is attached as Appendix 3. Essentially the officer making the request must check off a box and provide a name and badge number. If challenged, the City will argue that it has met its due diligence obligations, without asking police to breach any confidentiality requirements they may have, by confirming the information or material is required for police purposes.

Library Policies: Rights and Responsibilities

Policy Prohibitions	Vancouver	Calgary	Edmonton	Toronto	Mississauga	Ottawa	Niagara Falls	Windsor	Halifax
policy applies to wifi network as well		X	X						
policy denotes insecure wifi network	X	X							X
internet access policy	X	X	X		X				
damaging or modifying the library's computer equipment			X		X		X	X	X
installing and/or running programs	X	X			X		X	X	
infringe copy right			X			X		X	X
anything illegal*	X	X		X	X	X	X	X	
harassment, libeling or slandering of others			X						X
fraud or invasion or privacy			X						
gambling			X						
display or dissemination of hate literature, child pornography, literature for illicit drug use or obscene material		X	X		X	X	X		
display or dissemination of any material tending to deprive any person of his/her rights, to expose any dignity			X						
viewing pages displaying pornography			X						
commercial profit							X	X	
brutal, graphic and/or sexual violence			X						
creating or distributing spam mail messages			X		X		X		X
use of multiple cards and or use of other people's library cards	X		X				X	X	

x = expressly denoted in policy

* cities with x's in this box appear to encompass all prohibited activities outlined, and use it as a "catch all" prohibition

APPENDIX 2

1ST SESSION, 39TH LEGISLATURE, ONTARIO
57 ELIZABETH II, 2008

Bill 128

An Act to protect our children from sexual predators and exposure to electronic forms of sexual material by amending Christopher's Law (Sex Offender Registry), 2000 and other Acts

Mr. Martiniuk

Private Member's Bill

1st Reading	November 19, 2008
2nd Reading	
3rd Reading	
Royal Assent	

Printed by the Legislative Assembly of Ontario

1re SESSION, 39e LÉGISLATURE, ONTARIO
57 ELIZABETH II, 2008

Projet de loi 128

Loi visant à protéger nos enfants contre les prédateurs sexuels et contre l'exposition à des documents à caractère sexuel diffusés sous forme électronique en modifiant la Loi Christopher de 2000 sur le registre des délinquants sexuels et d'autres lois

M. Martiniuk

Projet de loi de député

1re lecture	19 novembre 2008
2e lecture	
3e lecture	
Sanction royale	

Imprimé par l'Assemblée législative de l'Ontario

EXPLANATORY NOTE

The Bill amends a number of Acts to protect minors from sex offenders or exposure to sexual material in electronic form.

Christopher's Law (Sex Offender Registry), 2000

The Bill amends the Act so that the sex offender registry will cover a person who, to the knowledge of the Ministry under the Act, is resident in Ontario and who is an offender with respect to a sex offence in a jurisdiction outside Canada if the Ministry considers the offence equivalent to a sex offence in Canada and if the regulations made under the Act prescribe the jurisdiction.

Subject to the limitations prescribed by the regulations made under the Act, any person, not just an employee of a police force or the Ministry as at present, is entitled, at no charge, to inspect the sex offender registry and to make copies of any part of the registry.

Education Act

Every school board is required to ensure that every school of the board has in place technology measures on all of the school's computers to which a person under the age of 18 years has access. The technology measures must do the following:

1. They must block access on the Internet to any material, including written material, pictures and recordings, that is obscene or sexually explicit or that constitutes child pornography.
2. They must block access to any form of electronic communication, including electronic mail and chat rooms, if the communication could reasonably be expected to expose a person under the age of 18 years to any material, including written material, pictures and recordings, that is obscene or sexually explicit or that constitutes child pornography.
3. They must block access to any site on the Internet or to any form of electronic communication, including electronic mail and chat rooms, if the school has not authorized users of the computers to access the site or the communication or if the site or the communication could reasonably be expected to contain material that includes personal information about a person under the age of 18 years.

A school is required to have a policy on who are authorized to use its computers to which a person under the age of 18 years has access and to monitor the use that persons under the age of 18 years make of those computers.

Public Libraries Act

The Bill amends the *Public Libraries Act* to make amendments that are similar to those that the Bill makes to the *Education Act*, except that the duties of a school board are those a board with respect to every library under its jurisdiction and the duties of a school are those of a public library.

NOTE EXPLICATIVE

Le projet de loi modifie plusieurs lois pour protéger les personnes mineures contre les délinquants sexuels ou contre une exposition à des documents à caractère sexuel diffusés sous forme électronique.

Loi Christopher de 2000 sur le registre des délinquants sexuels

Le projet de loi modifie la Loi de façon à ce que figure au registre des délinquants sexuels quiconque, à la connaissance du ministère visé par la Loi, réside en Ontario et est un délinquant à l'égard d'une infraction sexuelle commise dans le ressort d'une autorité législative de l'extérieur du Canada si le ministère estime que l'infraction équivaut à une infraction sexuelle au Canada et que les règlements pris en application de la Loi prescrivent l'autorité législative en question.

Sous réserve des restrictions prescrites par les règlements pris en application de la Loi, n'importe qui a le droit, et non pas seulement un employé d'un corps de police ou du ministère comme c'est le cas actuellement, d'examiner sans frais le registre des délinquants sexuels et d'en copier n'importe quelle partie.

Loi sur l'éducation

Les conseils scolaires doivent veiller à ce que chacune de leurs écoles ait mis en place, sur tous ses ordinateurs auxquels ont accès des personnes de moins de 18 ans, des mesures de protection technique qui doivent faire ce qui suit :

1. Bloquer l'accès sur Internet à des documents, notamment des écrits, des images et des enregistrements, qui sont obscènes ou sexuellement explicites ou qui constituent de la pornographie juvénile.
2. Bloquer l'accès à une forme de communication électronique, notamment le courrier électronique et les clavardoirs, dans le cas où il serait raisonnable de s'attendre à ce que cette communication expose des personnes de moins de 18 ans à des documents, notamment des écrits, des images et des enregistrements, qui sont obscènes ou sexuellement explicites ou qui constituent de la pornographie juvénile.
3. Bloquer l'accès à un site Internet ou à une forme de communication électronique, notamment le courrier électronique et les clavardoirs, si l'école n'a pas autorisé les utilisateurs des ordinateurs à y avoir accès ou dans les cas où il serait raisonnable de s'attendre à ce que ce site ou cette communication contienne des documents où figurent des renseignements personnels au sujet d'une personne de moins de 18 ans.

Les écoles doivent également adopter une politique permettant de déterminer qui est autorisé à utiliser les ordinateurs scolaires auxquels ont accès des personnes de moins de 18 ans et à surveiller l'usage que font ces personnes de tels ordinateurs.

Loi sur les bibliothèques publiques

Le projet de loi modifie la *Loi sur les bibliothèques publiques* pour y apporter des modifications semblables à celles qu'il apporte à la *Loi sur l'éducation*, sauf que les obligations d'un conseil scolaire sont celles d'un conseil à l'égard des bibliothèques relevant de sa compétence et les obligations des écoles sont celles des bibliothèques publiques.

Bill 128 **2008**

An Act to protect our children from sexual predators and exposure to electronic forms of sexual material by amending Christopher's Law (Sex Offender Registry), 2000 and other Acts

This Act amends or repeals more than one Act. For the legislative history of these Acts, see the Table of Consolidated Public Statutes – Detailed Legislative History on www.e-Laws.gov.on.ca.

Her Majesty, by and with the advice and consent of the Legislative Assembly of the Province of Ontario, enacts as follows:

CHRISTOPHER'S LAW (SEX OFFENDER REGISTRY), 2000

1. (1) The definition of "offender" in subsection 1 (1) of *Christopher's Law (Sex Offender Registry), 2000* is repealed and the following substituted:

"offender" means a person,

(a) who has been convicted of an offence described in clause (a), (b) or (c) of the definition of "sex offence" in this subsection,

(b) who has been found not criminally responsible of an offence described in clause (a), (b) or (c) of the definition of "sex offence" in this subsection on account of mental disorder, or

(c) who is resident in Ontario and who,

(i) has been convicted of an offence described in clause (d) of the definition of "sex offence" in this subsection, or

(ii) has been found not criminally responsible of an offence described in clause (d) of the definition of "sex offence" in this subsection on account of mental disorder; ("délinquant")

(2) If, on the day this subsection comes into force, subsection 1 (2) of *Christopher's Law (Sex Offender Registry) Amendment Act, 2008* is not in force, the definition of "sex offence" in subsection 1 (1) of the Act is amended by striking out "or" at the end of clause (b), by adding "or" at the end of clause (c) and by adding the following clause:

Projet de loi 128 **2008**

Loi visant à protéger nos enfants contre les prédateurs sexuels et contre l'exposition à des documents à caractère sexuel diffusés sous forme électronique en modifiant la Loi Christopher de 2000 sur le registre des délinquants sexuels et d'autres lois

Remarque : La présente loi modifie ou abroge plus d'une loi. L'historique législatif de ces lois figure aux pages pertinentes de l'Historique législatif détaillé des lois d'intérêt public codifiées sur le site www.lois-en-ligne.gouv.on.ca.

Sa Majesté, sur l'avis et avec le consentement de l'Assemblée législative de la province de l'Ontario, édicte :

LOI CHRISTOPHER DE 2000 SUR LE REGISTRE DES DÉLINQUANTS SEXUELS

1. (1) La définition de «délinquant» au paragraphe 1 (1) de la *Loi Christopher de 2000 sur le registre des délinquants sexuels* est abrogée et remplacée par ce qui suit :

«délinquant» Personne qui, selon le cas :

a) a été déclarée coupable d'une infraction visée à l'alinéa a), b) ou c) de la définition de «infraction sexuelle» au présent paragraphe;

b) a été déclarée criminellement non responsable d'une infraction visée à l'alinéa a), b) ou c) de la définition de «infraction sexuelle» au présent paragraphe pour cause de troubles mentaux;

c) réside en Ontario et, selon le cas :

(i) a été déclarée coupable d'une infraction visée à l'alinéa d) de la définition de «infraction sexuelle» au présent paragraphe,

(ii) a été déclarée criminellement non responsable d'une infraction visée à l'alinéa d) de la définition de «infraction sexuelle» au présent paragraphe pour cause de troubles mentaux. («offender»)

(2) Si, le jour de l'entrée en vigueur du présent paragraphe, le paragraphe 1 (2) de la *Loi de 2008 modifiant la Loi Christopher sur le registre des délinquants sexuels* n'est pas en vigueur, la définition de «infraction sexuelle» au paragraphe 1 (1) de la Loi est modifiée par adjonction de l'alinéa suivant :

(d) an offence in a jurisdiction outside Canada that is prescribed if, in the opinion of the ministry, the offence is equivalent to an offence described in clause (a), (b) or (c);

(3) On the later of the day this subsection comes into force and the day subsection 1 (2) of *Christopher's Law (Sex Offender Registry) Amendment Act, 2008* comes into force, the definition of "sex offence" in subsection 1 (1) of the Act is amended by striking out "or" at the end of clause (b.1), by adding "or" at the end of clause (c) and by adding the following clause:

(d) an offence in a jurisdiction outside Canada that is prescribed if, in the opinion of the ministry, the offence is equivalent to an offence described in clause (a), (b), (b.1) or (c);

2. Section 2 of the Act is amended by adding the following subsection:

Exception

(2) Nothing in subsection (1) requires the ministry to include in the sex offender registry information about a person described in clause (c) of the definition of "offender" in subsection 1 (1) unless the ministry has knowledge that the person is resident in Ontario.

3. Subsection 8 (1) of the Act is amended by striking out the portion before clause (a) and substituting the following:

Application of Act

(1) This Act applies to every offender anywhere in Canada or in a jurisdiction outside Canada that is prescribed who,

. . . . . .

4. (1) Subsection 10 (1) of the Act is amended by striking out "(2) and (3)" and substituting "(2), (3) and (3.1)".

(2) Section 10 of the Act is amended by adding the following subsection:

Access by public

(3.1) Subject to the prescribed limitations, if any, a person is entitled, at no charge, to inspect the sex offender registry and to make copies of any part of the registry if the person follows the prescribed procedure.

(3) Subsection 10 (4) of the Act is amended by striking out "(2) or (3)" and substituting "(2), (3) or (3.1)".

5. Section 14 of the Act is amended by adding the following clauses:

(a.1) prescribing a jurisdiction outside Canada for the purpose of clause (d) of the definition of "sex offence" in subsection 1 (1) and for the purpose of subsection 8 (1);

. . . . . .

d) d'une infraction commise dans le ressort d'une autorité législative de l'extérieur du Canada qui est prescrite si, de l'avis du ministère, l'infraction équivaut à une infraction visée à l'alinéa a), b) ou c).

(3) Le dernier en date du jour où le présent paragraphe entre en vigueur et du jour où le paragraphe 1 (2) de la *Loi de 2008 modifiant la Loi Christopher sur le registre des délinquants sexuels* entre en vigueur, la définition de «infraction sexuelle» au paragraphe 1 (1) de la Loi est modifiée par adjonction de l'alinéa suivant :

d) d'une infraction commise dans le ressort d'une autorité législative de l'extérieur du Canada qui est prescrite si, de l'avis du ministère, l'infraction équivaut à une infraction visée à l'alinéa a), b), b.1) ou c).

2. L'article 2 de la Loi est modifié par adjonction du paragraphe suivant :

Exception

(2) Le paragraphe (1) n'a pas pour effet d'exiger que le ministère inclue dans le registre des délinquants sexuels des renseignements concernant une personne visée à l'alinéa c) de la définition de «délinquant» au paragraphe 1 (1) à moins qu'il n'ait connaissance que la personne réside en Ontario.

3. Le paragraphe 8 (1) de la Loi est modifié par substitution de ce qui suit au passage qui précède l'alinéa a) :

Champ d'application de la Loi

(1) La présente loi s'applique aux délinquants, n'importe où au Canada ou dans le ressort d'une autorité législative de l'extérieur du Canada qui est prescrite, qui :

. . . . . .

4. (1) Le paragraphe 10 (1) de la Loi est modifié par substitution de «(2), (3) et (3.1)» à «(2) et (3)».

(2) L'article 10 de la Loi est modifié par adjonction du paragraphe suivant :

Accès par le public

(3.1) Sous réserve des restrictions prescrites, le cas échéant, toute personne a le droit d'examiner sans frais le registre des délinquants sexuels et d'en copier n'importe quelle partie à condition de suivre les modalités prescrites.

(3) Le paragraphe 10 (4) de la Loi est modifié par substitution de «(2), (3) ou (3.1)» à «(2) ou (3)».

5. L'article 14 de la Loi est modifié par adjonction des alinéas suivants :

a.1) prescrire une autorité législative de l'extérieur du Canada pour l'application de l'alinéa d) de la définition de «infraction sexuelle» au paragraphe 1 (1) et pour l'application du paragraphe 8 (1);

. . . . . .

(d.1) prescribing limitations and a procedure for the purpose of subsection 10 (3.1);

EDUCATION ACT

6. Section 230 of the *Education Act* is amended by striking out "or" at the end of clause (b), by adding "or" at the end of clause (c) and by adding the following clause:

(d) contravenes section 321, 322 or 323.

7. The Act is amended by adding the following Part:

PART XIII.2
PROHIBITING ACCESS TO ELECTRONIC FORMS OF SEXUAL MATERIAL

Blocking access to sexual material

321. (1) In this section,

"sexually explicit material" means material of which a principal feature or characteristic is the nudity or partial nudity of any person and that is designed to appeal to erotic or sexual appetites or inclinations.

Same

(2) A board shall ensure that every school of the board has in place technology measures on all of the school's computers to which a minor may have access that,

(a) block access on the Internet to any material, including written material, pictures and recordings, that is obscene within the meaning of subsection 163 (8) of the *Criminal Code* (Canada) or sexually explicit or that constitutes child pornography within the meaning of section 163.1 of the *Criminal Code* (Canada); and

(b) block access to any form of electronic communication, including electronic mail and chat rooms, if the communication could reasonably be expected to expose a minor to any material, including written material, pictures and recordings, that is obscene within the meaning of subsection 163 (8) of the *Criminal Code* (Canada) or sexually explicit or that constitutes child pornography within the meaning of section 163.1 of the *Criminal Code* (Canada).

Severability

(3) Technology measures that a school adopts under subsection (2) do not contravene that subsection if they comply with that subsection and, in addition, allow access on the Internet to material that does not contravene clause (2) (a) or allow access to any form of electronic communication that does not contravene clause (2) (b).

d.1) prescrire des restrictions et des modalités pour l'application du paragraphe 10 (3.1);

LOI SUR L'ÉDUCATION

6. L'article 230 de la *Loi sur l'éducation* est modifié par adjonction de l'alinéa suivant :

d) contrevient à l'article 321, 322 ou 323.

7. La Loi est modifiée par adjonction de la partie suivante :

PARTIE XIII.2
INTERDICTION D'ACCÈS À DES DOCUMENTS À CARACTÈRE SEXUEL SOUS FORME ÉLECTRONIQUE

Accès bloqué : documents à caractère sexuel

321. (1) La définition qui suit s'applique au présent article.

«documents sexuellement explicites» Documents dont une des caractéristiques principales est la nudité intégrale ou partielle d'une personne et qui sont conçus pour stimuler les appétits ou les tendances sexuels ou érotiques.

Idem

(2) Tout conseil veille à ce que chacune de ses écoles ait mis en place sur tous ses ordinateurs auxquels peuvent avoir accès des personnes mineures des mesures de protection technique qui :

a) d'une part, bloquent l'accès sur Internet à des documents, notamment des écrits, des images et des enregistrements, qui sont obscènes, au sens du paragraphe 163 (8) du *Code criminel* (Canada), ou sexuellement explicites ou qui constituent de la pornographie juvénile, au sens de l'article 163.1 du *Code criminel* (Canada);

b) d'autre part, bloquent l'accès à une forme de communication électronique, notamment le courrier électronique et les clavardoirs, dans le cas où il serait raisonnable de s'attendre à ce que cette communication expose des personnes mineures à des documents, notamment des écrits, des images et des enregistrements, qui sont obscènes, au sens du paragraphe 163 (8) du *Code criminel* (Canada), ou sexuellement explicites ou qui constituent de la pornographie juvénile, au sens de l'article 163.1 du *Code criminel* (Canada).

Dissociabilité

(3) Les mesures de protection technique qu'adopte une école en application du paragraphe (2) ne contreviennent pas à ce paragraphe si elles sont conformes à celui-ci tout en permettant l'accès sur Internet à des documents qui ne contreviennent pas à l'alinéa (2) a) ou à une forme de communication électronique qui ne contrevient pas à l'alinéa (2) b).

Blocking access to unauthorized material

322. (1) A board shall ensure that every school of the board has in place technology measures on all of the school's computers to which a minor may have access that block access to any site on the Internet or to any form of electronic communication, including electronic mail and chat rooms, if,

(a) the school has not authorized users of the computers to access the site or the communication; or

(b) the site or the communication could reasonably be expected to contain material that includes personal information within the meaning of the *Freedom of Information and Protection of Privacy Act* about a minor.

Policy for authorized access

(2) A board shall ensure that,

(a) every school of the board has a policy to determine what minors or class of minors are authorized to use the school's computers to access what sites on the Internet and what forms of electronic communication, including electronic mail and chat rooms;

(b) the policy described in clause (a) meets the requirements, if any, prescribed by the regulations; and

(c) every school of the board publishes a notice setting out the policy described in clause (a) in conspicuous places in the school, as the school determines and the regulations require.

Monitoring electronic access by minors

323. A board shall ensure that every school of the board,

(a) monitors the use by minors of any or all of the school's computers to access the Internet or any form of electronic communication, including electronic mail or chat rooms for the purpose of allowing the board to determine whether it has met its obligations under section 321 or 322; and

(b) has in place technology measures that permit the school to perform the monitoring described in clause (a).

Regulations

324. (1) The Minister may make regulations,

(a) specifying standards that technology measures must meet for a board to comply with its requirements in section 321, 322 or 323;

(b) prescribing or specifying anything that this Part describes as being prescribed or required in the regulations.

Accès bloqué : documents non autorisés

322. (1) Tout conseil veille à ce que chacune de ses écoles ait mis en place sur tous ses ordinateurs auxquels peuvent avoir accès des personnes mineures des mesures de protection technique qui bloquent l'accès à un site Internet ou à une forme de communication électronique, notamment le courrier électronique et les clavardoirs, si, selon le cas :

a) l'école n'a pas autorisé les utilisateurs des ordinateurs à avoir accès à ce site ou à cette forme de communication;

b) il serait raisonnable de s'attendre à ce que ce site ou cette communication contienne des documents où figurent des renseignements personnels au sens de la *Loi sur l'accès à l'information et la protection de la vie privée* au sujet d'une personne mineure.

Politique concernant l'accès autorisé

(2) Tout conseil veille à ce qui suit :

a) chacune de ses écoles adopte une politique permettant de déterminer quelles personnes mineures ou catégories de telles personnes sont autorisées à utiliser ses ordinateurs pour avoir accès à quels sites Internet ou à quelles formes de communication électronique, notamment le courrier électronique et les clavardoirs;

b) la politique visée à l'alinéa a) satisfait aux exigences éventuelles prescrites par les règlements;

c) chacune de ses écoles publie un avis énonçant la politique visée à l'alinéa a) à des endroits bien en vue dans l'école, selon ce que détermine l'école et ce qu'exigent les règlements.

Surveillance : accès électronique par les personnes mineures

323. Tout conseil veille à ce que chacune de ses écoles :

a) d'une part, surveille l'usage que font les personnes mineures de ses ordinateurs pour avoir accès à Internet ou à toute forme de communication électronique, notamment le courrier électronique et les clavardoirs, de façon à permettre au conseil de déterminer s'il a rempli les obligations que lui impose l'article 321 ou 322;

b) d'autre part, ait mis en place des mesures de protection technique qui lui permettent de procéder à la surveillance visée à l'alinéa a).

Règlements

324. (1) Le ministre peut, par règlement :

a) préciser les normes auxquelles doivent satisfaire les mesures de protection technique pour que les conseils se conforment aux exigences de l'article 321, 322 ou 323;

b) prescrire ou préciser tout ce que la présente partie mentionne comme étant prescrit ou exigé dans les règlements.

General or specific application

(2) A regulation made under this section may be of general application or specific to any person, persons, thing or things or class or classes in its application.

Classes

(3) A class described in the regulations made under this section may be described according to any characteristic or combination of characteristics and may be described to include or exclude any specified member, whether or not with the same characteristics.

PUBLIC LIBRARIES ACT

8. Part III of the *Public Libraries Act* is amended by adding the following sections:

Blocking access to sexual material

38.1 (1) In this section,

"sexually explicit material" means material of which a principal feature or characteristic is the nudity or partial nudity of any person and that is designed to appeal to erotic or sexual appetites or inclinations.

Same

(2) A board shall ensure that every library under its jurisdiction has in place technology measures on all of the library's computers to which a minor may have access that,

(a) block access on the Internet to any material, including written material, pictures and recordings, that is obscene within the meaning of subsection 163 (8) of the *Criminal Code* (Canada) or sexually explicit or that constitutes child pornography within the meaning of section 163.1 of the *Criminal Code* (Canada); and

(b) block access to any form of electronic communication, including electronic mail and chat rooms, if the communication could reasonably be expected to expose a minor to any material, including written material, pictures and recordings, that is obscene within the meaning of subsection 163 (8) of the *Criminal Code* (Canada) or sexually explicit or that constitutes child pornography within the meaning of section 163.1 of the *Criminal Code* (Canada).

Severability

(3) Technology measures that a library adopts under subsection (2) do not contravene that subsection if they comply with that subsection and, in addition, allow access on the Internet to material that does not contravene clause (2) (a) or allow access to any form of electronic communication that does not contravene clause (2) (b).

Portée générale ou particulière

(2) Les règlements pris en application du présent article peuvent avoir une portée générale ou ne s'appliquer qu'à des personnes, objets ou catégories particuliers.

Catégories

(3) Une catégorie visée dans les règlements pris en application du présent article peut être décrite selon n'importe quelle caractéristique ou combinaison de caractéristiques, et peut être décrite comme une catégorie incluant ou excluant tout membre précisé, que celui-ci soit doté ou non des mêmes caractéristiques.

LOI SUR LES BIBLIOTHÈQUES PUBLIQUES

8. La partie III de la *Loi sur les bibliothèques publiques* est modifiée par adjonction des articles suivants :

Accès bloqué : documents à caractère sexuel

38.1 (1) La définition qui suit s'applique au présent article.

«documents sexuellement explicites» Documents dont une des caractéristiques principales est la nudité intégrale ou partielle d'une personne et qui sont conçus pour stimuler les appétits ou les tendances sexuels ou érotiques.

Idem

(2) Le conseil veille à ce que chaque bibliothèque relevant de sa compétence ait mis en place sur tous ses ordinateurs auxquels peuvent avoir accès des personnes mineures des mesures de protection technique qui :

a) d'une part, bloquent l'accès sur Internet à des documents, notamment des écrits, des images et des enregistrements, qui sont obscènes, au sens du paragraphe 163 (8) du *Code criminel* (Canada), ou sexuellement explicites ou qui constituent de la pornographie juvénile, au sens de l'article 163.1 du *Code criminel* (Canada);

b) d'autre part, bloquent l'accès à une forme de communication électronique, notamment le courrier électronique et les clavardoirs, dans le cas où il serait raisonnable de s'attendre à ce que cette communication expose des personnes mineures à des documents, notamment des écrits, des images et des enregistrements, qui sont obscènes, au sens du paragraphe 163 (8) du *Code criminel* (Canada), ou sexuellement explicites ou qui constituent de la pornographie juvénile, au sens de l'article 163.1 du *Code criminel* (Canada).

Dissociabilité

(3) Les mesures de protection technique qu'adopte une bibliothèque en application du paragraphe (2) ne contreviennent pas à ce paragraphe si elles sont conformes à celui-ci tout en permettant l'accès sur Internet à des documents qui ne contreviennent pas à l'alinéa (2) a) ou à une forme de communication électronique qui ne contrevient pas à l'alinéa (2) b).

Blocking access to unauthorized material

38.2 (1) A board shall ensure that every library under its jurisdiction has in place technology measures on all of the library's computers to which a minor may have access that block access to any site on the Internet or to any form of electronic communication, including electronic mail and chat rooms, if,

(a) the library has not authorized users of the computers to access the site or the communication; or

(b) the site or the communication could reasonably be expected to contain material that includes personal information within the meaning of the *Freedom of Information and Protection of Privacy Act* about a minor.

Policy for authorized access

(2) A board shall ensure that,

(a) every library under its jurisdiction has a policy to determine what minors or class of minors are authorized to use the library's computers to access what sites on the Internet and what forms of electronic communication, including electronic mail and chat rooms;

(b) the policy described in clause (a) meets the prescribed requirements, if any; and

(c) every library under its jurisdiction publishes a notice setting out the policy described in clause (a) in conspicuous places in the library, as the library determines and the regulations require.

Monitoring electronic access by minors

38.3 A board shall ensure that every library under its jurisdiction,

(a) monitors the use by minors of any or all of the library's computers to access the Internet or any form of electronic communication, including electronic mail or chat rooms for the purpose of allowing the board to determine whether it has met its obligations under section 38.1 or 38.2; and

(b) has in place technology measures that permit the library to perform the monitoring described in clause (a).

Minister's regulations

38.4 (1) The Minister may make regulations,

(a) specifying standards that technology measures must meet for a board to comply with its requirements in section 38.1, 38.2 or 38.3;

(b) specifying anything that section 38.2 describes as being prescribed or required in the regulations.

Accès bloqué : documents non autorisés

38.2 (1) Le conseil veille à ce que chaque bibliothèque relevant de sa compétence ait mis en place sur tous ses ordinateurs auxquels peuvent avoir accès des personnes mineures des mesures de protection technique qui bloquent l'accès à un site Internet ou à une forme de communication électronique, notamment le courrier électronique et les clavardoirs, si, selon le cas :

a) la bibliothèque n'a pas autorisé les utilisateurs des ordinateurs à avoir accès à ce site ou à cette forme de communication;

b) il serait raisonnable de s'attendre à ce que ce site ou cette communication contienne des documents où figurent des renseignements personnels au sens de la *Loi sur l'accès à l'information et la protection de la vie privée* au sujet d'une personne mineure.

Politique concernant l'accès autorisé

(2) Le conseil veille à ce qui suit :

a) chaque bibliothèque relevant de sa compétence adopte une politique permettant de déterminer quelles personnes mineures ou catégories de telles personnes sont autorisées à utiliser ses ordinateurs pour avoir accès à quels sites Internet ou à quelles formes de communication électronique, notamment le courrier électronique et les clavardoirs;

b) la politique visée à l'alinéa a) satisfait aux exigences éventuelles prescrites par les règlements;

c) chaque bibliothèque relevant de sa compétence publie un avis énonçant la politique visée à l'alinéa a) à des endroits bien en vue dans la bibliothèque, selon ce que détermine la bibliothèque et ce qu'exigent les règlements.

Surveillance : accès électronique par les personnes mineures

38.3 Le conseil veille à ce que chaque bibliothèque relevant de sa compétence :

a) d'une part, surveille l'usage que font les personnes mineures de ses ordinateurs pour avoir accès à Internet ou à toute forme de communication électronique, notamment le courrier électronique et les clavardoirs, de façon à permettre au conseil de déterminer s'il a rempli les obligations que lui impose l'article 38.1 ou 38.2;

b) d'autre part, ait mis en place des mesures de protection technique qui lui permettent de procéder à la surveillance visée à l'alinéa a).

Règlements du ministre

38.4 (1) Le ministre peut, par règlement :

a) préciser les normes auxquelles doivent satisfaire les mesures de protection technique pour que le conseil se conforme aux exigences de l'article 38.1, 38.2 ou 38.3;

b) préciser tout ce que l'article 38.2 mentionne comme étant prescrit ou exigé dans les règlements.

General or specific application

(2) A regulation made under this section may be of general application or specific to any person, persons, thing or things or class or classes in its application.

Classes

(3) A class described in the regulations made under this section may be described according to any characteristic or combination of characteristics and may be described to include or exclude any specified member, whether or not with the same characteristics.

COMMENCEMENT AND SHORT TITLE

Commencement

9. This Act comes into force on the day it receives Royal Assent.

Short title

10. The short title of this Act is the *Christopher's Statute Law Amendment Act (Sex Offender Registry and Electronic Sexual Material), 2008*.

Portée générale ou particulière

(2) Les règlements pris en application du présent article peuvent avoir une portée générale ou ne s'appliquer qu'à des personnes, objets ou catégories particuliers.

Catégories

(3) Une catégorie visée dans les règlements pris en application du présent article peut être décrite selon n'importe quelle caractéristique ou combinaison de caractéristiques, et peut être décrite comme une catégorie incluant ou excluant tout membre précisé, que celui-ci soit doté ou non des mêmes caractéristiques.

ENTRÉE EN VIGUEUR ET TITRE ABRÉGÉ

Entrée en vigueur

9. La présente loi entre en vigueur le jour où elle reçoit la sanction royale.

Titre abrégé

10. Le titre abrégé de la présente loi est *Loi de 2008 modifiant des lois en ce qui a trait à la Loi Christopher (registre des délinquants sexuels et documents à caractère sexuel sous forme électronique)*.

APPENDIX 3

THE CORPORATION OF THE CITY OF MISSISSAUGA
RELEASE OF COMPUTER OR OTHER EQUIPMENT CONTAINING PERSONAL INFORMATION

Request to The Corporation of the City of Mississauga from the Peel Regional Police, Royal Canadian Mounted Police, Canadian Security Intelligence Service or Ontario Provincial Police for Release of Computer or other Equipment containing Personal Information for the Purposes of Law Enforcement as defined by the *MUNICIPAL FREEDOM OF INFORMATION AND PROTECTION OF PRIVACY ACT* (*MFIPPA*)

Release of the following Equipment is requested:

Employee/Customer Name (circle one) to which the personal information relates: _____

Location of Equipment (Division/Bldg): _____

Identify type of Equipment and Normal User of Equipment (if known/applicable):

Description of File(s)/Record(s): ALL FILES AND RECORDS CONTAINED IN COMPUTER/EQUIPMENT REFERRED TO ABOVE

TO BE COMPLETED BY THE POLICE OFFICER(S):

Name of Law Enforcement Agency: _____

Release of the Equipment identified above is requested in one of the following circumstances [tick one box]:

☐ 1. Release is to an institution or a law enforcement agency in Canada to aid an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result [MFIPPA sections 29(i)(b) and 32(g)][1]; or

☐ 2. In compelling circumstances affecting the health or safety of an individual [MFIPPA section 32 (h)][2]";

☐ 3. In compassionate circumstances, to facilitate contact with the next of kin or a friend of an individual who is injured, ill or deceased [MFIPPA section 32 (i)].

Occurrence No.:_____

The undersigned acknowledge(s) having taken the Equipment described above and further acknowledge(s) that such Equipment is the property of The Corporation of the City of Mississauga and that it will be returned when no longer required by the law enforcement agency named above.

Signature of Investigating Officer	Badge/Identification No.	Date
Signature of Investigating Officer	Badge/Identification No.	Date

TO BE COMPLETED BY CITY STAFF:

The Equipment of The Corporation of the City of Mississauga described above and containing personal information has been released in accordance with provisions allowing disclosure of information outside the City pursuant to MFIPPA section 32 (g) (h) or (i) as indicated above.

Signature of Staff Member Releasing Equipment	Name and Title	Date

Return completed Original to the DEPUTY CLERK, City of Mississauga, 300 City Centre Drive, 3rd[h] Floor Facade, Mississauga, Ontario L5B 3C1

---

[1] City staff must notify the Director of Human Resources immediately if a police request under circumstances #1 relates to a City Employee.

[2] If release is requested under circumstances #2, City staff must notify the individual immediately of the disclosure by letter mailed to his/her last known address.