The Intersection of Freedom of Information, Privacy Legislation and Library Services in Canadian Jurisdictions

Abstract: The intersection of freedom of information, privacy legislation and library services may be interpreted as the relation between two bodies (law and library) and how they influence one another directly and indirectly. This means library services can be shaped enormously by both federal and provincial freedom of information and privacy laws. We notice that there are cases in various Canadian courts involving disagreements concerning the rule of law in the fields of freedom of information and privacy with libraries. The combined effects of legislation and stronger library policies may make it more challenging for users to understand how to use shared library resources and services properly. For many libraries, this means operational policies and professional ethics codes have to be revised to strictly respect the users and employees' confidentiality rights. The research method used for this paper included a search of relevant Canadian court cases as case studies.

Keywords: Freedom of information; Privacy legislation; Canada

1. INTRODUCTION

The following introductory section presents basic concepts of privacy and freedom of information access rights. It begins with the international perceptions on privacy infringements, as many different countries have differing cultures on how they value personal information and privacy protection. The privacy and cultural differences concepts will link to the second part of this introductory section on the public privacy invasion case studies of the US National Security Agency (NSA) with Edward Snowden on the NSA's giant surveillance project. Furthermore, this paper discusses Canada's recently passed Bill C-51, which contains a provision on sharing information among federal government departments, which gives cause for serious privacy concerns. Then, we will provide insight into the legal logic model and the intersection of freedom of information right and privacy right with an essential keyword of "identifiable", when data can be used to identify someone. This legal thinking section will build a good foundation towards the following sections in this paper discussing the Organization for Economic Cooperation and Development (OECD) guidelines and Canadian legislation and case laws in privacy and freedom of information access.

PRIVACY AND CULTURAL DIFFERENCES

Countries value personal privacy differently, based on their own local cultures. For example, in Thai culture it is acceptable for a person to ask or publicly comment on someone's age, weight, and marital status even about someone you barely know. These kinds of comments are not perceived by Thai people as being inappropriate or rude.

Interestingly, instead, it is interpreted as a caring act. In Thailand, societies are structured upon collective social characteristics. Thai culture puts emphasis on being together as a group. The wall protecting personal information about one's physical appearance is not strongly constructed. Personal appearance is seen as a common group discussion topic. The same question is considered inappropriate in Western and Canadian cultures, however, where the cultures are fundamentally based on the individualistic social characteristics. There is a clear line defining personal matters, therefore questions or comments about someone's personal appearance are often avoided in public.

Remarkably, there is no consensus among Western countries about privacy and personal information protection. Research by James Q. Whitman (2004), a Yale University's comparative and foreign law professor stated that US law requires Americans to submit to extensive credit reporting. Merchants can access customers' entire credit records. Meanwhile the member states of the European Union consider credit reporting a serious violation of consumer data. Another interesting comparison by Professor Whitman finds that in Germany, many city parks legally allow nudity. In contrast nudity in public parks is not allowed by US law or accepted by American social norms.[1] These privacy examples in different cultures and countries should not be used to judge if one situation is better than another, but serve to illustrate the existence of privacy and cultural differences. Countries decide to set rules and laws based on their own historical, social, political, and economical circumstances.

PRIVACY SURVEILLANCE: FROM EDWARD SNOWDEN TO CANADA'S BILL C-51

In June 2013, Edward Snowden, a former US National Security Agency (NSA) computer specialist released information about the NSA's mass international secret surveillance project, spying particularly on foreign government leaders and also including all American personal communications on their phones and internet, using their advanced telecommunication technologies and infrastructures. Snowden's leak quickly went viral worldwide, across many news channels and social media. The fact that the NSA surveillance project had gone beyond their country's borders, became a very serious concern. In addition, Snowden claimed that the Chancellor of Germany, Angela Merkel's telephone was tapped along with many other country leaders during some important official meetings. The story of Snowden has caused people around the world to start asking questions about the safety of their own online personal information in the digital era. Does privacy really exist on the internet, telephones, and cellphones nowadays?

Linking what is happening in Canada recently, the government of Canada led by the Conservative Party of Canada has been attempting to pass the Bill C-51 with the short title of "Anti-terrorism bill" in the Parliament. At the time of writing this paper, Bill C-51 had already passed through all three readings in the House of Commons and the Senate.[2]

---

[1] Whitman, Jame Q. (2004) The two western cultures of privacy: dignity versus liberty. *Yale Law Journal* 133(6), 1151-1221

[2] Parliament of Canada, C-51:
http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&billId=6842344&View=0

The Act has now been given Royal Assent. Bill C-51 contains a bill within the bill, creating the *Security of Canada Information Sharing Act*. This Act will order 17 principal government institutions to disclose citizens' personal records held at those institutions to the federal government. The 17 institutions include:

1. Canada Border Services Agency
2. Canada Revenue Agency
3. Canadian Armed Forces
4. Canadian Food Inspection Agency
5. Canadian Nuclear Safety Commission
6. Canadian Security Intelligence Service
7. Communications Security Establishment
8. Department of Citizenship and Immigration
9. Department of Finance
10. Department of Foreign Affairs, Trade and Development
11. Department of Health
12. Department of National Defence
13. Department of Public Safety and Emergency Preparedness
14. Department of Transport
15. Financial Transactions and Reports Analysis Centre of Canada
16. Public Health Agency of Canada
17. Royal Canadian Mounted Police

Essentially, the Act provides the government with the legal right to create a new protocol for massive personal information surveillance. There are some concerns about the Act, particularly in term of its enormous scope. The personal information records listed inside the Act cover everything from personal health information to tax and financial data, allowing for any personal information gathered over the course of an individual Canadian's entire life to be shared. The second concern is the inclusion of the Communications Security Establishment in this list. This institution is equipped with modern computer network technologies and a team of IT experts.[3] They can make online surveillance happen without any difficulty which conjures up similarities to the National Security Agency and Edward Snowden case.

Undeniably, Canada has been facing issues with terrorism from domestic and international attacks. In one incident in October of 2014, a shooter fatally shot a soldier on Parliament Hill. Later, polices released the gunman's video to the public. The video shows that the shooter's anger was partly flued by Canada's involvements in the Iraq and Afghanistan wars and other political turmoils in the Middle-East. Moreover, there have been several police arrests and investigations linked to terrorist activities and terrorist

[3] Commmunications Security Establishment, What we do and why we do it: https://www.cse-cst.gc.ca/en/inside-interieur/what-nos

financial supports on Canada's soil. Such events no doubt served to encourage the Conservations Party of Canada to rush to pass Bill C-51. Opposition parties in the Parliament have been persuaded by the Bill's ability to protect safety for Canadians, especially on their own land. The Liberal Party of Canada has supported this Bill during the legislation process.[4] The official opposition, the New Democratic Party of Canada (NDP) however has voted against the Bill and now seeking for a petition to repeal it,[5] bolstered by public and scholarly community concerns about what will happen if the government uses this new power to accessing mass personal information for their own political agendas. It will be a long time before people truly realise how the government will use the citizens' personal information. However given the Canadian social characteristic of placing such a high value on privacy protection, it is somewhat unusual to see such a Bill that allows the government to infringe on the privacy of individuals pass in Canada.

LEGAL LOGIC MODEL OF FREEDOM OF INFORMATION AND PRIVACY RIGHTS

The *Access to Information Act* (Right) and the *Privacy Act* (Right) are unified codes. They are truly interconnected. Starting by looking at Canadian laws, citizens have a right to access records that contain personal information about themselves held by the government. These records having been collected and maintained by government are referred to in the legal context as "public sector" records. These records may be in the possession of federal government institutes, departments, or ministries. The law also covers documents held by provincial government organisations like municipalities and local agencies and boards. The *Access to Information Act* (Right) is meant to provide freedom of information access rights to every Canadian. Personal information documents collected, used, and disclosured by private sector organisations however are based on individual consent. Personal information such as names, address, and age, needed if, for instance, someone were opening a bank account, cannot be gathered by private sector organisations without the individual's consent. A bank would have to ask the applicant to consent to the bank's privacy policies regarding the collect, use, and disclose of this information to a third party before the bank could collect it. Importantly, all citizens also have the right to ask the private enterprises to withdraw their previously given consents in order to put an end to their personal information being collected by the private sector's systems and operations. This consent withdrawn is legally permitted and protected by Canada's *Personal Information Protection and Electronic Documents Act (PIPRD)*.[6]

The *Access to Information Act* (Right), however, contains certain exemptions blocking the disclosure of certain public and private sectors documents from the public or a third party. The exemptions are for specific categories such as cabinet records, government defence records, individual safety records, personal privacy records, etc. To provide some further examples, documents such as medical history records, employment

[4] Liberal Party of Canada, Remarks by Liberal Party of Canada leader Justin Trudeau on Bill C-51: https://www.liberal.ca/remarks-by-justin-trudeau-on-bill-c-51/

[5] New Democratic Party of Canada, Petition: Repeal Bill C-51: http://www.ndp.ca/repeal-c-51

[6] CanLII, Personal Information Protection and Electronic Documents Act, SC 2000, c 5: http://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/latest/sc-2000-c-5.html

history records, financial records and general records that have information on personal religion belief, sexual orientation, residential address, or even full names, may be kept private. These are considered as the sensitive private information, as the given information could be used to identify a particular individual. Thus, there are some concerns that there may be negative consequences if a person has been identified through public and private sector records. A person's security and well-being may be in danger should someone be able to access and use their personal information. Below is a figure of a legal logic model created by the authors to visualize the interconnection of freedom of information right and privacy protection right.

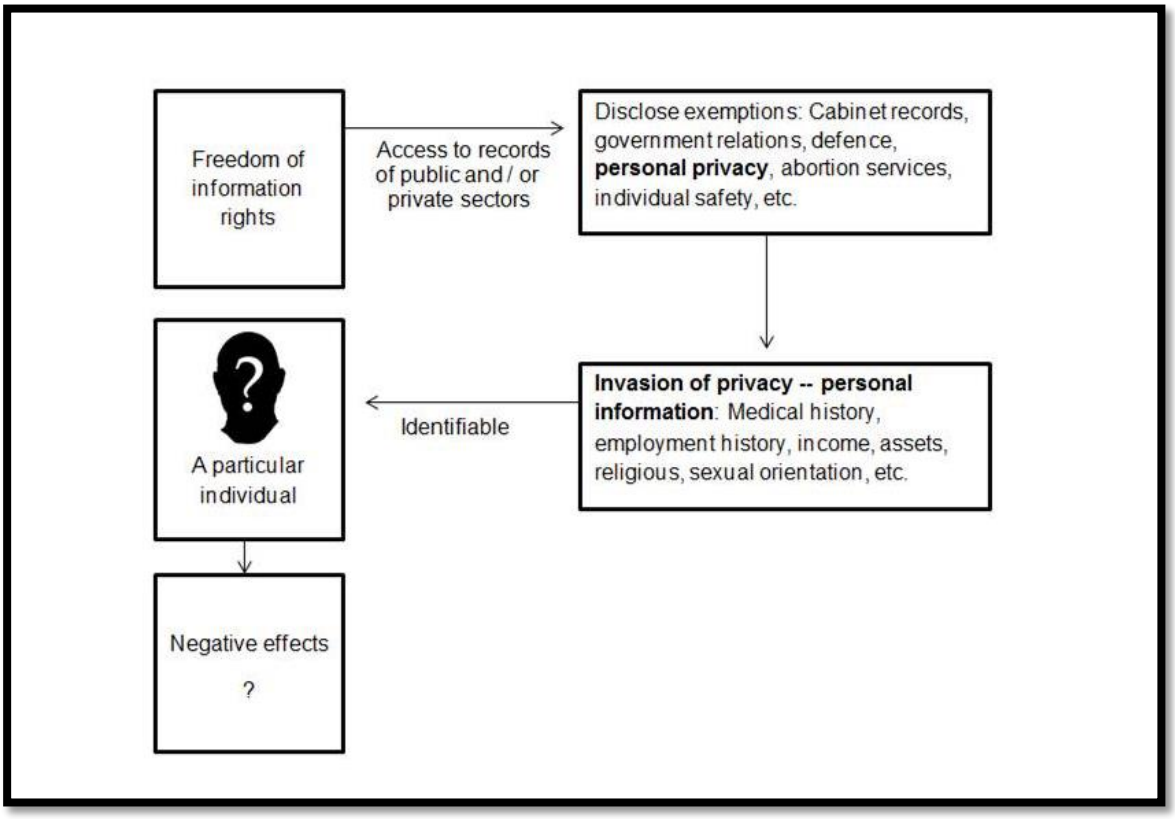

Figure 1: Legal logic model of freedom of information and privacy rights

2. GLOBAL TRENDS IN FREEDOM OF INFORMATION AND PRIVACY

This section aims to investigate the international regulation of privacy information, which may inspire a baseline for privacy information protection in the library environment. With this in mind, we will review the Organization for Economic Cooperation and Development (OECD)'s documents that establish guidelines for privacy information. Our objective is to verify how libraries could (re)shape their relationship with their users based on these guidelines.

OECD GUIDELINES

The OECD is a multilateral organisation which aims to promote economic and social well-being around the word.[7] Because of this, the OECD establishes cooperation between its members through coordinated actions. Common problems demand similar solutions in order to foster a harmonized development. For this purpose, the OECD issues binding guidelines that its memberships should internalize to implement such coordinated actions.

Among other questions, the OECD has realized that information technology has had an impact economic and social development. Indeed, new technologies have allowed for the implementation of planned administration through the personal data management of citizens (census). Even vendors have started to create consumer profiles to increase their sales.[8] Privacy, economic and social development have become competing values. Because of this, the OECD has issued some guidelines in order to accommodate privacy protection as well as social and economic development.[9]

Those guidelines have created a pattern for personal data mining. The narrative of personal data protection has been framed as citizens´ right to control their personal information. With the issuance of the OECD's Guidelines,[10] there has been a policy convergence[11] around the denominated Fair Information Practice Principles (FIPPs) which aims to ensure that individuals self-manage their privacy.[12] Indeed, the Guidelines'

[7] The Organisation for Economic Co-operation and Development (OECD), About the OECD: http://www.oecd.org/about/

[8] OECD, OECD guidelines on the protection of privacy and transborder flows of personal data: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[9] Ibid

[10] Ibid

[11] Gellman, Robert. Fair information practices: A basic history: http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf

[12] Solove, Daniel (2013) Privacy self-management and the consent dilemma. *Harvard Law Review* 126, at 1882.

eight principles[13] centre the individual as its core normative element, wherein they should be given notice about the collection, use, and disclosure of their personal information, where they can then choose to grant consent for it or not.

DATA MINIMIZATION APPROACH TO OECD GUIDELINES

Most importantly, all libraries should have a privacy policy. As it was said before, data subjects should be given notice about the collection, use and disclosure of their personal information. Privacy policies are able to establish such communication in order to inform the patrons about how their personal information is handled in the library environment. Among other questions, privacy policies should clarify the confidentiality of library records, whether third parties are involved in the personal data management, what security safeguards are adopted, etc. With this information, patrons can manage their personal information since they can evaluate the risks against their privacy based on the terms and conditions of the privacy policy. Privacy policies are, therefore, the first step in empowering data subject to control their personal information, performing, ultimately, the informational self-determination according to the OECD´s guidelines. However, personal data protection is not only the library users' responsibility. Rather it is a shared responsibility which requires the cooperation those who manage the personal information. Libraries also have the responsibility of protecting patron´s privacy. For instance, they can become less harmful to personal data management by adopting the principle of data minimization.

Libraries should minimize the amount of data stored. They should only manage any patron personal information that is strictly necessary[14] to provide their services. Whether the objective is to associate the patron to the borrowed books, few pieces of information (identifiers) are necessary to create this connection and consequently, manage the library business. Beyond this quantitative approach, the collection should also be qualitatively less invasive. For instance, a social security number is sensitive information. Hence, other identifiers should replace them if they can precisely individualize someone (driver's licence, student number etc.). By this approach, the data subject privacy will always be more protected.

In conclusion, privacy policies should only be a mechanism to collect patrons 'consent with regard to the traditional concept of library services. Patrons should specifically and undoubtedly consent for the management of their personal information when it is necessary to implement additional services. Only by this approach will patron's consent

[13] The eight principles: a) Collection Limitation Principle; b) Data Quality Principle; c) Purpose Specification Principle; d) Use Limitation Principle; e) Security Safeguards Principle; f) Openness Principle; g) Individual Participation Principle; h) Accountability Principle. The principles a, c, d, e, g made express reference to the individual in order to enforce themselves the protection of their personal information.

[14] Poullet, Y. (2010) "About the e-privacy directive: Towards a third generation of data protection legislation?" in *Data Protection in a Profiled World*. New York, Springer Books, 2007. at 27

be an efficient mechanism for true privacy protection, in accordance with the OECD´s guidelines.

The OECD guidelines establish minimum standards for privacy protection which may be adopted in the library environment around the world. On one hand, these guidelines should shape the relationship between libraries and their patrons. Library users should have more control over their personal information, particularly against the new library services that demand more invasive personal data management. The OECD guidelines have properly addressed both questions in order to accommodate privacy, as well as economic and social development as competing values. Such approach should not be different in the library environment since the access to the information and privacy are similarly colliding interests. For this reason, the OECD guidelines may provide inspiration to revise the library policies.

3. CANADIAN LEGISLATIONS AND CASE LAWS

In this section, we will see how the privacy and freedom of information laws in the federal and provincial legislations coincide. All provinces have used the federal laws as the blueprint and some provinces have added some unique sections into their own legislations. The samples of provincial case laws reviewed in this section show that some cases are only related to the legality of privacy right, while some cases are concerned with both privacy and freedom to information access. The case samples used here only involving the public sectors. No private sector case is discussed here because the focus on this paper is on library services, which in Canada are operated through government funding and public supports.

FEDERAL AND PROVINCIAL LEGISLATIONS

Personal information and privacy protection are under both federal and provincial legislations. In the federal legislation, two major Acts are related to the individual privacy right: 1. *The Privacy Act*, 2. The *Personal Information Protections and Electronic Documents Act (PIPEDA)*. The major differences of those two Acts are that the *Privacy Act* is being used to protect individual personal information that is being collected, used, and disclosed at the public sector organisations (Government and Crown corporations). *PIPEDA*, however, is deals with public personal information under the control and operation of private sector organisations. *PIPEDA* was initially suggested by the European Commission as a Canadian Act as the Commission wanted to ensure their citizens' personal information was strongly protected in Canada, especially when dealing with the transection of digital economy and information exchange in communication technologies that the Europeans do online business transactions with many Canadian companies to receive services and products, such as in the banking industry and for tourism purposes; therefore there is a need to for Canadian federal legislation to protect EU citizens' personal information. Lastly, *PIPEDA* has developed to cover more aspects of Canadian privacy rights within the private sector.

For provincial legislation, each province governs their own legislation relating to citizens privacy protection. In this area of law, most of the provinces use a legislative context similar to the federal legislation. The provincial legislation for Alberta (*Personal Information Protection Act*), British Columbia (*Personal Information Protection Act*) and Quebec (*An Act Respecting the Protection of Personal Information in the Private Sector*) are deemed substantially similar to *PIPEDA*. The legislation for Ontario (*Personal Health Information Protection Act*), New Brunswick (*Personal Health Information Privacy and Access Act*), and Newfoundland (*Personal Health Information Act*) are considered equivalent to *PIPEDA* when it comes to health information. And finally, Alberta and British Columbia is unique in having specific sections for employee information.

CASE LAWS IN FREEDOM OF INFORMATION AND PRIVACY

The Province of Alberta: Parkland Regional Library director vs. An Employee.[15]

The case hearing occurred at the Alberta Information and Privacy Commission. The Library director had a keystroke logging program installed on a newly hired employee's workstation computer to record all keyboard interactions. The employee was not informed about the shadowing program. The Library director argued in front of the judges that the recorded data was to be used to evaluate the employee's productivity during his initial probationary period. The employee, upon discovering the software, was concerned about an invasion into his own privacy and personal information as the employee has also been permitted to use the workstation computer for his personal online banking during non-working hours. His financial information was recorded. Section 33 of the *Freedom of Information and Protection of Privacy Act,* R.S.A. 2000, C. F-25 allows public bodies to collection "personal information" if it is "information relates directly to and is necessary for an operating program or activity of the public body." The judge ruled that the library director's actions, in representing a public body (the library network) violated section 33 of the act, citing that the keystroke information was not necessary for the management of that public body. The judge added that there are other sufficient ways to evaluate the employee's work performance without using the keystroke logging program. The employee's online banking information that has been recorded on the keystroke program was considered as a privacy infringement.

[15] *Re Parkland Regional Library* (24 June 2005), F2005-003, online: AOIPC <www.oipc.ab.ca/downloads/documentloader.ashx?id=2123>.

The Province of British Columbia: Vancouver Public Library Board vs. CUPE.[16]

This case had been judged by the British Columbia Collective Agreement Arbitration Awards. In the case, a library employee has been on sick leave with unpaid benefit for eighteen months. The library had a policy in place requiring that they have some access to information about the employee's medical condition, achieved through a consultation between the employee's doctor and the employer's occupational physician. This consultation would allow for the two doctors to set out any restrictions, modifications and guidelines necessary during the employee's absence or in preparation for their return to work. During the long period of the employee's absence, he had only submitted , doctor's notes to the Library management, generally stating that the employee could not return to work, but continually refused to sign the medical release form, citing privacy concerns. The Union representing this employee tried to claim in the court that the employee should be entitled to return to work without any restrictions and the employee's general physician notes were enough to use as supporting evidential documents. The judge concluded that the employer could not impose a "blanket" requirement to fill out the form on its employees. However, the judge found that the non-specific doctors' notes provided by the employee did not provide a reasonable amount of information to the employer and ordered that the employee, in consultation with his doctor and lawyer make an initial judgement of the information to be forwarded to the employer.

The Province of Ontario: Toronto Public Library Board vs. A Library Member. [17]

A member of the public who officially has been banned from all properties of the Toronto Public Library due to an action committed towards another library patron. The banned library user made a request to access all records of the Toronto Public Library Board that contain his own personal information as every Canadian has the right and freedom to access information about themselves holding at public sectors. The Toronto Public Library presented the banned patron with a two page document titled as "Investigation of Reinstatement Request Report" which contains the requester's personal information. The document detailed the altercation which had previously occurred between the requester and another patron, which has led to his official exclusion from all properties of the Toronto Public Library. Inside the report, the personal information of the second patron involved in the altercation, particularly the legal full name had been removed to protect this individual's privacy and safety. However, the requester claimed that all information should be uncovered. This argument was not supported by the Ontario Information and Privacy Commissioner. The judge concluded that the Toronto Public Library Board's respond to the requester was the right action.

[16] *Vancouver Public Library Board v Canadian Union of Public Employees, Local 391 (Gulay Grievance),* [2008] BCCAAA 24, 93 CLAS 16.

[17] Toronto Public Library Board (Re), 2012 CanLII 38906 (ON IPC), online: OIPC <http://canlii.ca/t/fs0ls>.

The Province of Quebec: The National Library and Archives of Québec vs. A Library User.[18]

An information access application has been submitted to the Information Access Commissioner from an experienced lawyer who was also a university professor and writer, requesting to obtain the original documents of the Quebec Royal Commission meetings on the Wilbert Coffin case investigation. The documents were being kept at the Quebec's National Archives at Rimouski. The Library rejected the applicant's request to access the full documents of the Royal Commission, stating at that said documents were classified as closed materials and not to be viewed by the public. The Coffin case is a historically controversial Franco-Canadian murder case. In 1953, Mr. was charged with the murder of three American tourists from Pennsylvania in Gaspésie, Québec. Mr. Coffin was hanged. After his capital punishment, new evidence and independent research were published suggesting that Mr. Coffin was likely innocent. The Information Access Commissioner concluded that the documents be released with all names of witnesses and their identifiable personal information censored to respecting the witnesses' privacy and security.

LESSONS LEARNED

CASES	LESSONS LEARNED
The Province of Alberta: Parkland Regional Library director vs. An Employee.	If a public body is seeking to track the productivity of their employees, they should consider the collection of the employee's personal information may not be deemed as necessary to the operation of that public body and may be a violation of the employee's privacy.
The Province of British Columbia: Vancouver Public Library Board vs. CUPE.	When creating policies concerning employee medical leave, a library may consider the extent of information they may require as well as what sort of privacy implications this information could lead to. Furthermore, this case shows that providing next to no information is not necessarily justified in the face of privacy concerns.
The Province of Ontario: Toronto Public Library Board vs. A Library Member.	Though a patron may legally request any information the library may hold about themselves, that does not negate other

[18] *X v Bibliothèque et archives nationales du Québec* (10 December 2007), 06 10 38, online: QCAI <http://www.cai.gouv.qc.ca/documents/CAI_DSJ_061038de07w.pdf>.

	patron's rights to privacy. Having a good library policy in place, clearly stating that patrons should have a reasonable expectation of the confidentiality of their information.
The Province of Quebec: The National Library and Archives of Québec vs. A Library User.	Libraries can sometimes run into conflicts with the collection they hold and providing access to that collection, in matters of confidentiality.

4. RECOMMENDATIONS

From the background and case review in this paper the following recommendations are made for libraries about how they can support privacy protection.

1. Carefully study the third's party information disclosure of the publishers of any products to which a library is planning to subscribe, especially the online collections. User's information is systematically required to authorise online access for each individual. The database systems with internet access gathers large personal information automatically such as IP address, computer operation system, internet provider, and current location.

2. Educate and raise awareness about privacy protections for employees. This can be accomplished in part by compulsory training on privacy issues. Samples of privacy attack scenarios based on real work situations in the libraries should be debated. The training can be offered as a workshop or an online tutorial.

3. Offer workshops to library users about the necessary knowledge and skills to safely use online collections, internet, computers, and technologies at libraries to protect their privacy and personal information. Libraries also can feature a privacy data protection day/week with hand-on activities and informal lectures.

4. Publicly display library's privacy policies for users to be aware of the scope of library procedures regarding personal data. The privacy policies can be disseminated with posters or the policies on displayed library's website. Banks' privacy policies on websites can be used as the excellent example for libraries.

5. Promote privacy practitioners as a think tank in libraries. Library management teams should establish a privacy working group or committee to meet regularly and provide suggestions when a privacy conflict involving the library occurs in the future.

6. Use privacy risk assessment procedures in library projects. The privacy committee should conduct an internal privacy risk assessment on projects and services. The privacy committee should have a special authority to pause a project in which they

think the personal information is not being properly treated until the project's privacy risk assessment has been fully conducted and received an official approval from the Library director to continue the work. The privacy risk assessment can help the library to prepare if there is a litigation happening after the project has been launched to the public. In Canada by law, people have right to place a privacy complaint and grievance at the Ombudsman and the Information and Privacy Commissioners. Libraries can use the privacy risk assessment report to declare that the project is not unlawful. The report can show that public privacy has been carefully reviewed with the law.

7. Officially apply and rigorously exercise the privacy practice rules in the professional codes of ethics to all library personnel.

CONCLUSION

There is obviously an intersectional relationship between the legal aspects of freedom of information, privacy rights and library services. The world is being challenged with invasions of personal data, especially when the modern telecommunication tools are being used to spy people's privacy. Canada is not excluded regarding to the recently proposed Bill C-51. This Bill is claiming to be used to protect public security but it comes along with provisions for mass personal data surveillance. To focus on library services, Canadian provincial cases have shown that library privacy is a legal issue mixing with many other matters such the labour law (British Columbia case), police investigation (Québec case), inappropriate usage of technologies in the library administration (Alberta case), and individual library user demands (Ontario case). From this review the authors have proposed seven recommendations how libraries can support the user privacy protection. From now on, we should expect to hear more stories about personal data infringements in library communications as libraries are moving more and more to the online environment. There are new privacy challenges that libraries have never experienced. The best we can do is to prepare for unpredictable privacy and freedom of information access crisis. A key recommendation is the risk assessment, which will absolutely be a great practice for libraries worldwide in solving the new crisis created by privacy issues.

Footnotes:

[1] Whitman, Jame Q. (2004) The two western cultures of privacy: dignity versus liberty. *Yale Law Journal* 133(6), 1151-1221
[2] Parliament of Canada, C-51: http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&billId=6842344&View=0
[3] Commmunications Security Establishment, What we do and why we do it: https://www.cse-cst.gc.ca/en/inside-interieur/what-nos
[4] Liberal Party of Canada, Remarks by Liberal Party of Canada leader Justin Trudeau on Bill C-51: https://www.liberal.ca/remarks-by-justin-trudeau-on-bill-c-51/
[5] New Democratic Party of Canada, Petition: Repeal Bill C-51: http://www.ndp.ca/repeal-c-51

[6] CanLII, Personal Information Protection and Electronic Documents Act, SC 2000, c 5: http://www.canlii.org/en/ca/laws/stat/sc-2000-c-5/latest/sc-2000-c-5.html
[7] The Organisation for Economic Co-operation and Development (OECD), About the OECD: http://www.oecd.org/about/
[8] OECD, OECD guidelines on the protection of privacy and transborder flows of personal data: http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[9] Ibid
[10] Ibid
[11] Gellman, Robert. Fair information practices: A basic history: http://www.bobgellman.com/rg-docs/rg-FIPShistory.pdf
[12] Solove, Daniel (2013) Privacy self-management and the consent dilemma. *Harvard Law Review* 126, at 1882.
[13] The eight principles: a) Collection Limitation Principle; b) Data Quality Principle; c) Purpose Specification Principle; d) Use Limitation Principle; e) Security Safeguards Principle; f) Openness Principle; g) Individual Participation Principle; h) Accountability Principle. The principles a, c, d, e, g made express reference to the individual in order to enforce themselves the protection of their personal information.
[14] Poullet, Y. (2010) "About the e-privacy directive: Towards a third generation of data protection legislation?" in *Data Protection in a Profiled World*. New York, Springer Books, 2007. at 27
[15] *Re Parkland Regional Library* (24 June 2005), F2005-003, online: AOIPC <www.oipc.ab.ca/downloads/documentloader.ashx?id=2123>.
[16] *Vancouver Public Library Board v Canadian Union of Public Employees, Local 391 (Gulay Grievance),* [2008] BCCAAA 24, 93 CLAS 16.
[17] Toronto Public Library Board (Re), 2012 CanLII 38906 (ON IPC), online: OIPC <http://canlii.ca/t/fs0ls>.
[18] *X v Bibliothèque et archives nationales du Québec* (10 December 2007), 06 10 38, online: QCAI <http://www.cai.gouv.qc.ca/documents/CAI_DSJ_061038de07w.pdf>.

Biographies:

Ms. Margo Jeske (BA, MLS), Director, Brian Dickson Law Library, University of Ottawa

Margo Jeske has a bachelor's degree in French translation (Queen's University) and a master's degree in Library Science (Western University). She worked for several years in federal government departments and agencies and at the Library of Parliament, before joining the Brian Dickson Law Library, University of Ottawa as the Library Director. Margo is an active member of the Canadian Association of Law Libraries (CALL) and sits on the Law Libraries Section of the International Federation of Library Associations (IFLA).

Mr. Channarong Intahchomphoo (BA, MIS, E-Business PhD Student), Law Librarian (Replacement), Brian Dickson Law Library, University of Ottawa

Channarong Intahchomphoo holds a bachelor's degree (Chiang Mai University, Thailand) and an English/French bilingual master's degree (University of Ottawa, Canada) in Information Studies. Currently, Channarong is a replacement law librarian at the Brian Dickson Law Library, University of Ottawa. His fields of research and current projects are information and law, information organisations and new technology,

human-computer interaction: cross-cultural aspects, and social media for e-business and e-marketing. Channarong is also pursuing a doctorate in E-Business with the research topic of “Cross-Cultural Social Media Usage and Interaction in E-Business” at the Faculty of Engineering, University of Ottawa, Canada.

Ms. Emily Landriault (BA, MIS), Copyright Services Librarian, Brian Dickson Law Library, University of Ottawa

Emily Landriault holds a bachelor’s degree in English (University of Guelph) and a master’s degree in Library Studies (Dalhousie University). She has worked at legislative libraries, with time spent both at the Library of Parliament and at the Ontario Legislature. She came to the University of Ottawa as a reference librarian at the Brian Dickson Law Library and recently moved into a position as the Copyright Services Librarian for the university. Emily is an active member of the Canadian Association of Law Libraries (CALL) and serves as the treasurer for the National Capital Association of Law Librarians (NCALL).

Mr. Bruno Ricardo Bioni (LLB, LLM candidate), Visiting Researcher at the University of Ottawa’s Faculty of Law from São Paulo University, Brazil and Fellowship of São Paulo Research Foundation.

Master’s degree candidate at the Law Faculty of São Paulo University, Brazil. His research endeavors focus on personal data protection, especially about the implications of data subject’s consent to implement an effective legal framework. Bruno is a fellowship of the Research Support Foundation of São Paulo/FAPESP. His current research project have received two grants from FAPESP, one of them is for his 2014 visiting researcher opportunity at the Canada Research Lab for Law & Technology of the University of Ottawa. At the same year, he was the first place prize winner of a monograph competition which was organized by Brazilian Institute of Consumer Law & Policy. His winning monograph addressed about the interrelation between the duty of information and data subject’s consent in order to ensure a real personal data protection in the Brazilian context.