Lawful Access Legislation, Its Risks and Why Libraries Must Care

Brent Roe
Canadian Association of Research Libraries
Ottawa, Ontario, Canada

&

Jeannie Bail
Queen Elizabeth II Library
Memorial University of Newfoundland
St. John's, Newfoundland and Labrador, Canada

Session: 166 — *Master of contents or How to win the battle over freedom in cyberspace?* — Free Access to Information and Freedom of Expression (FAIFE) with Copyright and other Legal Matters (CLM)

Abstract:

This paper will briefly describe the development of "lawful access" legislation in Canada, both in the context of "non-cyber" investigative powers and controls on them, as well as in the context of post 9/11-terrorism concerns. It will look at the privacy concerns about the current Canadian bill—and inquire as to what privacy rights we cede to Internet Service Providers (ISPs) even without legislation. And finally, it will consider any direct effect on libraries of the legislation and the responsibility that library associations might nevertheless assume for raising awareness of privacy issues in increasing surveillance of Internet activities.

Introduction

Libraries and library associations work to favour broad access to many kinds of information and so promote the growth of the open access movement and work to limit the overreach of copyright protections. Libraries and their associations also endeavour to avoid the sharing of information—in the sense of information that would reveal the

reading or research interests of library patrons. In the Internet age, this extends also to a concern for the protection of the privacy of the users of their computers, library systems and online content. Because, however, those uses cannot be entirely separated from the non-library-related Internet activities of individuals, and because library-related Internet activity may be as easily traced, legally or otherwise, as other Internet activities of an individual, library associations have been developing positions around Internet and telecommunications privacy that are more general than ones concerning only library-related Internet activity.

This paper is a brief exploration of an Internet and telecommunications privacy issue that is of interest to libraries and library associations in many countries, but which has a current timeliness in Canada in the context of the recent introduction in Parliament of a bill with serious privacy concerns. The topic is "lawful access" and a question that library associations will want to pose for themselves is whether and under what circumstances they want to comment on, or even actively oppose, similar legislation out of their traditional concern for the privacy of the reader.

What Lawful Access Is

"Lawful Access" is a term that refers to the legally sanctioned access to information about a person's identity or activity on the Internet or on cellular phone networks, or even real-time interception of a person's activity, normally by law enforcement agencies. As defined by the Government of Canada, it sounds like a routine and vaguely comforting concept:

> Lawful Access is an important and well-established technique used by law enforcement and national security agencies to conduct investigations. In the context of telecommunications in Canada, it consists of the interception of communications and search and seizure of information carried out pursuant to legal authority….[1]

As defined on some civil society websites, the term may take on a rather more negative connotation:

> "Lawful Access" is the deceptively innocuous term given to the government's attempts to expand its power to spy on Internet activity. It does so by providing

[1] *Lawful Access-Consultation Document*, online: Department of Justice. <http://justice.gc.ca/eng/cons/la-al/a.html>.

new ways by which law enforcement and other state agents can lawfully access and intercept online activity and information.[2]

As the Internet and wireless telecommunications technologies and services have expanded over the last two decades, these tools have been used to facilitate the planning and execution of criminal activity as well as legal and beneficial activity. Governments and police forces have thus sought the legal and technical means to be able to monitor activity, to identify users, and investigate or prevent specific crimes.

Insofar as a democratic government will require legislative permission and public support for such monitoring of private activities, governments have generally cited public safety concerns such as the online sexual exploitation of children (e.g., in child pornography) and international terrorism as major targets for the necessary "lawful access" legislation. The most recent Canadian bill introduced on this topic was, in fact, entitled the *Protection of Children from Internet Predators Act* even though there was little provision in the bill specific to the protection of children. Aside from these more sensational crimes, lawful access provisions may also be helpful for the investigation of drug trafficking, smuggling, Internet and telemarketing fraud, price fixing and money laundering.[3]

Governments (generally their intelligence and antitrust agencies) and police forces may well have a legitimate need for lawful access abilities to fight crime that occurs or is facilitated online or over cellular telephone networks, but without strict controls and oversight, those abilities can be used also to monitor or control political opponents or even to commit crimes of a more personal nature on the part of a corrupt police officer or other official.

Lawful Access beyond Canada

Most developed countries have some form of lawful access legislation in place. In many cases, these laws are more invasive or require less judicial oversight than the measures recently proposed by the Canadian government. Some of the laws that are especially relevant as comparators are those in the United Kingdom, the United States, and Australia.

---

[2] *Lawful Access*, online: Canadian Internet Policy and Public Interest Clinic (CIPPIC) <http://cippic.ca/en/lawful-access>.

[3] *Government Review of Lawful Access Laws Includes the Competition Act*, online: Competition Bureau <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/eng/00404.html>.

In the United Kingdom, the *Regulation of Investigatory Powers Act* (RIPA) was passed in 2000 and has been broadened since.[4] RIPA allows various government and law enforcement agencies to demand from an Internet service provider (ISP) or a telecommunication service provider (TSP) access to records of a customer's communication transactions without notification of the customer for a range of purposes. And, in certain circumstances, it allows surveillance of all of the communication of an ISP/TSP. It allows for demands that ISPs/TSPs install interception capability and to demand encryption keys, and permits detailed monitoring of an individual's Internet activities.

In the United States, the *Communication Assistance for Law Enforcement Act* (CALEA) was passed in 1994 to require interception capability on telecommunication providers, but has been expanded since to cover ISPs as well.[5] In 2001, the *Uniting (and) Strengthening America (by) Providing Appropriate Tools Required (to) Intercept (and) Obstruct Terrorism Act* (USA PATRIOT Act) was passed, which gave sweeping powers to law enforcement agencies to perform surveillance activities on the communication and online activities of subjects, partly by amending other applicable laws.[6]

In Australia, the *Telecommunications Act* of 1997 allows for the requirement of interception capability and the assistance of the TSP/ISP with the interception.[7] Among other provisions, it also sets out the kinds of information that can be requested about a subscriber and allows this information to be placed in a database.

Christopher Parsons in a 2012 report summarizes the problems for personal privacy and civil liberties that some of these laws have occasioned.[8] He also summarizes the very broad and invasive powers currently being considered in France. It should be noted that most European countries have endorsed or ratified the Council of Europe's *Convention on Cybercrime*, which aims at coordinating investigative techniques

---

[4] *Regulation of Investigatory Powers Act 2000*, online: The National Archives <http://www.legislation.gov.uk/ukpga/2000/23/contents>.

[5] *Communications Assistance for Law Enforcement Act of 1994 (CALEA)*, online: AskCALEA <http://www.askcalea.net/calea/>.

[6] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, online: U.S. Government Printing Office <http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm>

[7] *TELECOMMUNICATIONS ACT 1997*, online: Commonwealth Consolidated Acts <http://www.austlii.edu.au/au/legis/cth/consol_act/ta1997214/>.

[8] Christopher Parsons, *Lawful Access and Data Preservation/Retention: Present Practices, Ongoing Harm and Future Canadian Policies* (2012). online: <http://www.christopher-parsons.com/blog/wp-content/uploads/2012/02/Lawful-Access-Report-v.2.2Final.pdf>.

(including Internet surveillance) and harmonizing laws in signatory countries.[9] [10] An irony of all these examples is that the countries noted are normally seen as generally protective of individual liberties. Clearly, there is little to suggest that more authoritarian regimes are more careful not to trespass on the privacy of their citizens.

Developing countries, whatever their governments' political leanings, may have different issues than lawful access. As Barbara Jones points out, in much of the less-developed world, the question of Internet privacy is hardly raised: the much larger concern is simply Internet access.[11]

Brief History of Lawful Access in Canada

Lawful access legislation in Canada has been relatively slow to materialize, mainly because of a series of minority governments that have failed to pass the various bills that they have proposed on account of those governments' falling, and national general elections being called (whereby any government bills "die on the order paper").

Since the 1970s, there has been provision in the *Criminal Code of Canada* for interception of communications (e.g., telephone wiretapping) and by the 1990s there was also provision for the search and seizure of computers systems. In 1984, these provisions in Canadian law spread beyond the *Criminal Code*, when national security intelligence responsibilities were removed from the Royal Canadian Mounted Police (RCMP), and given to a new agency, the Canadian Security Intelligence Service (CSIS); the *CSIS Act* also now contained such provisions. Aside from regular police forces (primarily among these the RCMP) and CSIS, the Competition Bureau would also make use of new lawful access provisions by way of the *Competition Act*.

Canada was a non-member participant in the discussions that led to the creation of the Council of Europe's *Convention on Cybercrime*, which was opened for signing in November 2001, with Canada as an original signatory, and which came into force in 2004. Partly with the goal of being in a position to achieve Canadian parliamentary ratification of the *Convention on Cybercrime*, the Liberal majority government of the time

---

[9] *Convention on Cybercrime,* online: Council of Europe <http://conventions.coe.int/Treaty/en/Treaties/html/185.htm>.

[10] *Signatory Treaty, Convention on Cybercrime*, online: Council of Europe <http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=&CL=ENG>.

[11] Barbara M. Jones, "Chapter 2: Libraries, Technology, and the Culture of Privacy A Global Perspective" (2010) 46:8 Library Technology Reports 8-9. online: <http://alatechsource.metapress.com/content/v3563n566p8mp031/>.

launched a public consultation on the matter in 2002, but did not, in the end, introduce a bill.[12]

After the general election of 2004, a Liberal minority government was formed and a lawful access bill (the *Modernization of Investigative Techniques Act* ["MITA"], Bill C-74) was introduced late in 2005.[13] This bill called for both the installation of the means to intercept real-time communication on Internet and telecommunication service provider networks, and for the ability of law enforcement officials to demand from those service providers identifying information on service subscribers without a judicial warrant. With the fall of the Liberal minority government not long after the introduction of MITA, the bill died on the order paper.

The new minority Conservative government, elected in 2006, did not introduce a new lawful access bill. That said, a Liberal Member of Parliament introduced a "private member's bill" (Bill C-416) in 2007 that contained the MITA content.[14] As private member's bills rarely pass into law in Canada, especially bills of opposition Members of Parliament, this bill received only first reading. The Conservative minority government fell in 2008, but was re-elected, again as a minority government, the same year. The same Liberal Member of Parliament as before (Ms. Marlene Jennings) re-introduced her private member's bill early in 2009, this time as Bill C-285.[15] Again, this bill only received "first reading."

The Conservative government was not to be outdone on the lawful access front by an opposition backbencher. As a part of a broader effort to operationalize in legislation a strong "law and order" agenda, this government introduced in June 2009 two lawful access bills, Bill C-46, the *Investigative Powers for the 21st Century Act*, and Bill C-47, the *Technical Assistance for Law Enforcement in the 21st Century Act*.[16] [17] The first of these would add to the list of offences covered by the *Criminal Code* a number of

---

[12] *Lawful Access - Consultation Document*, online: Department of Justice <http://www.justice.gc.ca/eng/cons/la-al/a.html#itm3>.
[13] *Bill C-74*, online: Parliament of Canada <http://www.parl.gc.ca/HousePublications/Publication.aspx?Pub=Bill&Doc=C-74&Language=E&Mode=1&Parl=38&Ses=1>.
[14] *Private Member's Bill C-416*, online: Parliament of Canada <http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&billId=2701217>.
[15] *Private Member's Bill C-285*, online: Parliament of Canada <http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&billId=3627149>.
[16] *Bill C-46*, online: Parliament of Canada <http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&billId=3997477>.
[17] *Bill C-47*, online: Parliament of Canada <http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&billId=3997619>.

offences relying on modern computing and telecommunication technology, provided language around preservation demands and orders and production orders, and proposed conditions for warranting the use of a transmission data recorder and a tracking device in investigations. The second, like the earlier Liberal bills, called for the installation of interception capability in computing and telecommunication networks, and the ability of law enforcement agencies to demand subscriber information from a service provider. These bills, however, got little further to passing into law than earlier bills because at the end of 2009, the Conservative government prorogued Parliament, which means that all government bills, again, die on the order paper.

In November 2010 the same government introduced three new lawful access bills: Bill C-50, the *Improving Access to Investigative Tools for Serious Crimes Act*; Bill C-51, the *Investigative Powers for the 21st Century Act*; and Bill C-52, the *Investigating and Preventing Criminal Electronic Communications Act*.[18] [19] [20] Bills C-51 and C-52 were similar to the earlier Bills C-46 and C-47. C-50 was to add a number of new or extended powers, allowing the use of interception of communications together with a search warrant, requiring an annual reporting of interceptions and the notification of individuals after interception, allowing for the use of a telephone number recorder without a warrant and for a longer period than before, and extending the maximum period of use of a tracking device. As it happened, this minority Conservative government also fell in the spring of 2011, so these bills also died on the order paper when an election was called.

On May 2, 2011, the Conservatives were elected with a small majority, the first majority government in Canada in power since mid-2004. As the Conservative government was determined to finally pass the range of anti-crime law that had been frustrated by the previous prorogation and election, the new Minister of Public Safety, Mr. Vic Toews, introduced an omnibus crime bill (Bill C-10, the *Safe Streets and Communities Act*) that incorporated nine earlier separate crime-related bills, but, to the surprise of many and with no explanation from the government, did not contain the lawful access bills.[21] It was assumed by some commentators that the government suspected that including the lawful access bills would have proven an impediment to the passage of the other less

---

[18] *Bill C-50*, online: Parliament of Canda <http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&billId=4729969>.
[19] *Bill C-51*, online: Parliament of Canada <http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&billId=4740078>.
[20] *Bill C-52*, online: Parliament of Canada <http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&billId=4740136>.
[21] *Bill C-10*, online: Parliament of Canada <http://www.parl.gc.ca/LegisInfo/BillDetails.aspx?Language=E&Mode=1&billId=5120829>.

controversial parts of the omnibus crime bill. However, the stage was now set for a new introduction of lawful access legislation in Canada.

Bill C-30 Overview

Controversial from the start, Bill C-30, officially long-titled *An Act to enact the Investigating and Preventing Criminal Electronic Communications Act and to amend the Criminal Code and other Acts*, was given its first reading in the House of Commons of Canada on Valentine's Day (a day celebrating romantic love), February 14, 2012. This is somewhat ironic, considering how little love the bill garnered from both the general public and policy-makers and followers. Sponsored by the same Minister of Public Safety, Mr. Toews, the bill was given the short title *Protecting Children from Internet Predators Act*, despite, as noted, there being almost no mention of either children or Internet predators. Mr. Toews created an uproar when he infamously stated that critics of the bill either stood with the Conservative Party "or with the child pornographers."[22]

As written, the purpose of Bill C-30 is "to ensure that telecommunications service providers have the capability to enable national security and law enforcement agencies to exercise their authority to intercept communications and to require telecommunications service providers to provide subscriber and other information, without unreasonably impairing the privacy of individuals, the provision of telecommunications services to Canadians or the competitiveness of the Canadian telecommunications industry."[23] In sum, Bill C-30 gives the power to law enforcement organization heads (and the Commissioner of Competition) to designate "any employee of his or her agency... whose duties are related to protecting national security or to law enforcement" to obtain subscriber information, including name, address, telephone number, IP address and email address, from Internet and telecommunications service providers without a warrant.[24] Thus, someone making an anonymous comment on a website could be linked to personal information held by an ISP. Currently, while ISPs can voluntarily provide this information, they are not mandated by law to do so. However, the current laws do not seem to impede police ability to fight crime effectively since the Minister of Public Safety was unable to recall a single instance where this bill would have made a difference in a crime that had taken place.[25]

---

[22] S. Chase & B. Curry, "Tories stung by e-privacy backlash" *The Globe and Mail* (16 February 2012).
[23] *Bill C-30*, online: Parliament of Canada <http://www.parl.gc.ca/HousePublications/Publication.aspx?Language=E&Mode=1&DocId=5380965>.
[24] *Ibid.* See Sections 16(1) and 16(3).
[25] Michael Geist, *Vic Toews' Lawful Access Deception* (12 December 2011), online: <http://www.michaelgeist.ca/content/view/6196/159/>.

In addition to the disclosure requirement, Bill C-30 also includes two other major prongs: surveillance and new police powers.[26] The surveillance prong requires ISPs to install technology that would make real-time surveillance possible, in addition to establishing regulatory requirements such as the disclosure of employees involved with surveillance activities. Compliance with these technological infrastructure and regulatory requirements is bound to be costly - a recent estimate is pegged at roughly 80 million dollars.[27] The new police powers would facilitate access to the surveillance data and include three new warrants: transmission warrants (to retrieve information), preservation orders (to retain information), and production orders (to force disclosure of preserved information).[28]

After Bill C-30 was introduced, it was immediately criticized by individuals, privacy advocates and civil liberties groups as overly intrusive and another example of the state's increasing employment of Internet surveillance. Federal and provincial Privacy Commissioners strongly objected as well, citing the bill as "an unjustified violation of privacy rights."[29] Even the Conservative Prime Minister, Mr. Stephen Harper, has shown signs of uneasiness with the bill (and perhaps with Mr. Toews himself), the government position being that it is "prepared to accept a broad range of changes."[30] Bill C-30 was quickly referred to the House of Commons Public safety Committee For study—before second reading in Parliament and with no clear timeline, an unusually ignoble fate for a government bill.

While it was most unusual for the Harper government to flinch in the face of adverse public opinion, its attitude isn't entirely surprising, given that the current Conservative government and party appear to have general concerns with privacy intrusion by government, recently making the controversial decisions to eliminate the mandatory long-form national census due to concerns over requiring disclosure of personal information and to scrap the non-restricted (long-gun) Canadian Firearms Registry, mandating also the destruction of the Registry records.

---

[26] Michael Geist, *Everything You Always Wanted to Know About Lawful Access, But Were (Understandably) Afraid to Ask* (13 February 2012), online: <http://www.michaelgeist.ca/content/view/6316/125/>.

[27] "Online surveillance bill setup costs estimated at $80M" (22 February 2012), online: CBC News: <http://www.cbc.ca/news/politics/story/2012/02/22/pol-lawful-access-costs.html>.

[28] *Ibid*.

[29] J. Ibbitson, "How the Toews-sponsored Internet surveillance bill quietly died; For all intents and purposes, Bill C-30, the Internet surveillance legislation sponsored by Public Safety Minister Vic Toews, is dead" *The Globe and Mail* (15 May 2012).

[30] *Chase & Curry*, *supra* note 22.

At present, the feeling is that the current bill will not reappear and that if the Conservative government still wants to introduce lawful access legislation, it will have to start over.[31] Specifically, some of the main criticisms of the bill are that personal information could be obtained without a person's knowledge or consent; that personal information would be disclosed without any oversight by the courts; that most ISPs already disclose information when asked by law enforcement officials (so there is no need to legislate this); that a former Conservative Public Safety Minister of Canada, Mr. Stockwell Day, pledged not to introduce legislation enabling police to obtain information from ISPs without a warrant due to privacy expectations; and that there would be a substantial amount of money required to implement the surveillance reporting infrastructure as required by legislation, in addition to new technical capabilities to allow for real-time surveillance. It appears that the problems with the bill are numerous, and it is likely that the latest effort to pass lawful access legislation into Canadian law will not succeed. However, given its decade-long contemplation in Canada, the issue of lawful access has captured the attention of many citizens and policy makers; for a future iteration of a lawful access bill to be successful, more careful consideration will need to be given to balancing the need for law enforcement information gathering against citizen privacy concerns.

Civil Society Concerns with Lawful Access Legislation

In the U.S. and Canada, many civil society groups such as the Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic (CIPPIC), Canadian Journalists for Free Expression (CJFE), American Civil Liberties Union (ACLU), Electronic Privacy Information Center (EPIC) and the Electronic Frontier Foundation (EFF) have been working to confront the threat to privacy rights that increased government surveillance in electronic communications poses. These organizations have been instrumental in terms of serving as information clearinghouses, advocacy groups, and mobilizers in the fight against the erosion of privacy rights in the digital age. CIPPIC states that it is "concerned that attempts to update 'lawful access' capabilities are far from targeted and will have serious detrimental impact on Canadians' civil liberties," although it does concede that lawful access legislation has been carefully crafted to avoid challenges to the Canadian *Charter of Rights and Freedoms*, which has a standard of a "reasonable expectation of privacy."[32] Only a Supreme Court challenge would reveal whether particular lawful access legislation could pass this test. The CJFE, which is a part of IFX - the International Free Expression Exchange, runs programs for journalists to "protect

[31] *Ibbitson*, *supra* note 29.

[32] *Lawful Access*, online: Canadian Internet Policy and Public Interest Clinic (CIPPIC) <http://www.cippic.ca/en/lawful-access>.

and defend free expression both in Canada and around the world."[33] To exemplify the joint work that is often performed by libraries and civil liberties groups, the CJFE was presented with the Canadian Library Association's Award for the Advancement of Intellectual Freedom in Canada in 2007. The CJFE publishes an annual *Review of Free Expression in Canada*. The 2011/2012 edition examined privacy and anonymity on the Internet and cyber surveillance. In a featured article, Dr. Michael Geist, the Canada Research Chair of Internet and E-commerce Law at the University of Ottawa, writes that Bill C-30, with its surveillance technology infrastructure requirements, sends the message to companies that specialize in commercial surveillance equipment that "Canada is open for 'Big Brother Inc.' business."[34]

In the U.S., both EPIC and EFF are well-known for their privacy rights activism. EFF, founded in 1990, works primarily in the court system and Congress on issues relating to rights in cyberspace, including free speech, fair use, and privacy. It has a keen interest in the global Internet, and examines issues in the international arena as well. As part of its education-based work, EFF empowers individuals, and advises on how to evaluate and protect against the threat of state surveillance through its Surveillance Self-Defense (SSD) Project. Like the American Library Association (ALA), the SSD Project advocates creating a data retention and destruction policy as a first and best defense against surveillance.[35] The EFF underscores the importance of having checks and balances in government powers - to balance law enforcement concerns against Constitutional civil liberties like privacy. This highlights one of the most problematic issues with Bill C-30: there is little consideration given to oversight and monitoring of the agencies authorized to request and obtain sensitive personal information. Under the *USA PATRIOT Act*, one must be presented with a subpoena for search and seizure. Bill C-30 grants the power to obtain personal information without a warrant, giving rise to possible information leaks and fishing expeditions. Established in 1994, EPIC's mission is to focus public attention on "emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values."[36] It primarily serves as a clearinghouse and publisher of information on various privacy issues, ranging from air travel to workplace privacy. The ACLU has listed "Surveillance & Privacy" as one of its trending issues, and has also characterized the post-9/11 security measure activities as "dragnet surveillance" that

---

[33] *Faq | Cjfe*, online: Canadian Journalists for Free Expression (CJFE) <http://www.cjfe.org/about_us/faq>.

[34] Michael Geist, *The Price of Peeking* in *CJFE's 2011/2012 Review of Free Expression in Canada*, online: <http://www.cjfe.org/resources/features/20112012-review-free-expression-canada-launched-world-press-freedom-day>.

[35] *Develop a Data Retention and Destruction Policy | EFF Surveillance Self-Defense Project*, online Electronic Frontier Foundation (EFF) <https://ssd.eff.org/your-computer/protect/retention>.

[36] *About EPIC*, online: Electronic Privacy Information Center (EPIC) <http://epic.org/epic/about.html>.

affects innocent people and undermines their rights to "privacy and the freedoms of speech, association, and religion."[37]

Implications of Lawful Access Legislation for Libraries

Privacy has long been recognized as a fundamental value of libraries. The Canadian Library Association (CLA) approved in 1987 a *Position Statement on Citizen Access to Information Data Banks - Right to Privacy*, stating that, as policy, "...names of library users not be released to any person, institution, association or agency for any reasons save as may be legally required by Federal or Provincial Laws."[38] The statement underscores the importance of privacy, and further comments on the "fundamental right" of users' privacy by restricting access to personal information.[39] Likewise, the ALA has long affirmed a right to privacy, and is at the forefront of privacy rights advocacy work in the United States. Its Office of Government Relations and Committee on Legislation have been involved with many legislative debates, including the *USA PATRIOT Act*, the *Electronic Computer Privacy Act* (EPCA) and the *Computer Assistance for Law Enforcement Act* (CALEA).[40] In its Interpretation of the Library Bill of Rights, it is said that "confidentiality is crucial to freedom of inquiry" and "(w)hen users recognize or fear that their privacy or confidentiality is compromised, true freedom of inquiry no longer exists."[41] On the global level, the International Federation of Library Associations and Institutions (IFLA) recognizes the right to privacy in its 2002 *Internet Manifesto*: "Libraries and information services should respect the privacy of their users and recognize that the resources they use should remain confidential."[42]

One of the major implications of lawful access legislation, in addition to increased advocacy work performed by library associations, is how libraries can protect users and educate them on privacy issues. After the *USA PATRIOT Act* was passed in the name of fighting terrorism after the 9/11 attacks, libraries became required by law to supply

---

[37] *Surveillance & Privacy - Recent Court Cases, Issues and Articles*, online: American Civil Liberties Union (ACLU) <http://www.aclu.org/national-security/surveillance-privacy>.

[38] *Citizenship Access to Information Data Banks - Right to Privacy*, online: Canadian Library Association (CLA) <http://www.cla.ca/AM/Template.cfm?Section=Position_Statements&Template=/CM/ContentDisplay.cfm&ContentID=3034>.

[39] *Ibid*.

[40] *Privacy & Surveillance*, online: American Library Association (ALA) <http://www.ala.org/advocacy/privacyconfidentiality>.

[41] *Privacy: An Interpretation of the Library Bill of Rights*, online: ALA <http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy>.

[42] *The IFLA Internet Manifesto*, online: International Federation of Library Associations (IFLA) <http://www.ifla.org/publications/the-ifla-internet-manifesto>.

library records under Section 215 of the *Act*, if requested by an authorized authority.[43] In addition, increased surveillance tactics were approved, including the expansion of wiretap surveillance to Internet and electronic communication. In Vermont state, library technologist Ms. Jessamyn West created signs for her public library, including "Q. How can you tell when the FBI has been in your library? A. You can't. The "Patriot" Act makes it illegal for us to tell you if our computers are being monitored: be aware!"[44] The ALA has advised libraries to review their retention and access policies of data that could potentially contain personal information.[45] The rationale behind this advice being that one can't find what one doesn't have. As an outreach tool, ALA created *Privacy Revolution*, a web site developed to educate and inform users on privacy issues. The web site emphasizes the library's role in privacy issues, stating "(l)ibrarians feel a professional responsibility to protect the right to search for information free from surveillance. Privacy has long been the cornerstone of library services in America."[46] Currently, it is too early to predict what strategies Canadian libraries will implement to protect users if far-reaching lawful access legislation is implemented, but there are plenty of examples to draw on from U.S. libraries in the aftermath of the adoption of the *USA PATRIOT Act*.

In her article "Libraries, Technology and the Culture of Privacy," Barbara Jones makes the argument that although privacy has been identified as an international core value to libraries, problems exist in embracing privacy rights in a digital environment for the global library community, namely "vastly different legal and regulatory environments, different levels of national technological development, different cultural interpretations for the meaning of privacy and the clash of priorities and values - transparency vs. privacy."[47] Jones also makes the point that privacy as a library issue hasn't been sufficiently promoted and urges librarians to make the issue more demanding of attention via campaigns that appeal more to the emotions, cautioning that the loss of privacy is incremental.[48]

---

[43] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, online: U.S. Government Printing Office <http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/html/PLAW-107publ56.htm>.

[44] Jessamyn West, *Five Technically Legal Signs for Your Library*, online: Librarian.net <http://www.librarian.net/technicality.html>.

[45] *Guidelines for Librarians on the USA PATRIOT Act: What to do before, during and after a 'knock at the door?,* online: ALA <http://www.ala.org/advocacy/sites/ala.org.advocacy/files/content/advleg/federallegislation/theusapatriotact/patstep.pdf>.

[46] *Privacy Revolution*, online: ALA <http://www.privacyrevolution.org/>.

[47] Jones, *supra* note 11 at 8-9.

[48] *Ibid.* at 12.

Tension for Library Associations: Comment Broadly or Stick to "Their Own" Concerns?

As discussed above, libraries have been very sensitive to the issue of privacy of the reader. Many library associations around the world have statements on this matter. Some, such as that of the Japan Library Association, are very explicit about this: "Libraries shall not reveal a reader's record of reading, except upon warrant issued by a competent judicial officer provided in the Constitution (Article 35)…Libraries shall not violate a readers' privacy by revealing any record of using the library in addition to the record of reading".[49] It is for this reason that librarians in the United States have shown so much opposition to the USA PATRIOT Act: it embodies a very clear threat to the privacy of the reader inasmuch as library records can be demanded with minimal judicial review and without the possibility of alerting affected library patrons. The American Library Association statement is quite clear: "The American Library Association (ALA) opposes any use of governmental power to suppress the free and open exchange of knowledge and information or to intimidate individuals exercising free inquiry…ALA considers that sections of the USA PATRIOT ACT are a present danger to the constitutional rights and privacy rights of library users."[50]

But the question must be posed as to whether libraries and library associations should or will oppose problematic lawful access legislation when it does not directly or clearly pose a threat to the privacy of the (library) reader, that is, when the threat of a compromise of privacy is at the level of society and not at the level, in any specific sense, of users of libraries.

In Canada, Bill C-30, like its forerunner bills, specifically excludes libraries from the direct application of most of the terms of the bill, even though many libraries are *de facto* ISPs (Section 5 specifies that only Section 24 will apply: the necessity to give law enforcement upon request information about the communication systems and services that they provide). It is not clear whether this exception was made to respect the particular sensitivities around privacy in libraries and other such organizations or was a recognition of the likely high cost of making a network interception-ready. Nevertheless, it will likely have blunted some library association concerns with the bill.

---

[49] *Statement on Intellectual Freedom in Libraries,* online: Japan Library Association <http://www.jla.or.jp/portals/0/html/jiyu/english.html>.

[50] *The USA Patriot Act in the Library*, online: ALA <http://www.ala.org/offices/oif/ifissues/usapatriotactlibrary>.

Libraries and library associations in Canada will want to consider the role they wish to play in educating users and members about lawful access privacy concerns, and advocating against potentially harmful lawful access legislation. Librarians and the directors of their associations may not, as citizens, like a particular piece of legislation, but they may be tempted to leave it to other civil society organizations like the ACLU and EFF to oppose it. We do note that the Canadian Library Association did vote a resolution of opposition in 2003 to the concept of expanded lawful access legislation in Canada[51] and did submit a brief to the 2002-2003 public consultation on the topic; no other library associations submitted briefs to the consultation.[52]

In the Canadian case, particularly strong opposition to the creation of new lawful access legislation has come from the federal and provincial Privacy Commissioners, who have been united and outspoken over the whole of the last decade in their opinion that new legislation is unnecessary, and that judicial oversight remains crucial for even seeking subscriber information from ISPs and TSPs.[53] [54] [55] The Privacy Commissioners have a great deal of respect as independent "watchdogs" of government and business in Canada in defence of citizen privacy (the current federal Privacy Commissioner, Ms. Jennifer Stoddart, has also successfully taken Facebook to task on its privacy policies).[56] It would be relatively easy for library groups in Canada to simply reference, in their communications about lawful access legislation, the concerns or at least the statements of the Privacy Commissioners, even if they do not wish to discuss directly matters that do not specifically concern libraries. Many countries, unfortunately, do not have such authorities on the topic that are recognized both by government and society more broadly.

---

[51] *2003 Resolutions of the 58th Annual General Meeting*, online: CLA <http://www.cla.ca/AM/PrinterTemplate.cfm?Section=AGM_2003>.

[52] *Summary of Submissions to the Lawful Access Consultation*, online: Department of Justice <http://www.justice.gc.ca/eng/cons/la-al/sum-res/index.html>.

[53] Jennifer Stoddart, *Letter to the Minister of Public Safety Vic Toews* (26 October 2011), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/media/nr-c/2011/let_111027_e.asp#contenttop>.

[54] *Letter to Public Safety Canada from Canada's Privacy Commissioners and Ombudspersons on the current 'Lawful Access' proposals* (9 March 2011), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/media/nr-c/2011/let_110309_e.asp>.

[55] George Radwanski, *Letter to the Minister of Justice and the Attorney General of Canada* (5 November 2002), online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/media/le_021125_e.asp>.

[56] Office of the Privacy Commissioner of Canada, News Release, "Privacy Commissioner: Facebook shows improvement in some areas, but should be more proactive on privacy when introducing new features" (4 April 2012), online: <http://www.priv.gc.ca/media/nr-c/2012/nr-c_120404_e.asp>.

Canadians, as well as citizens of other countries, will also want to ask themselves whether the greatest threats to their Internet and telecommunication privacy might not be so much the actions of government and law enforcement as the actions of their ISPs/TSPs as well as their very own personal behaviors. In the discussion of lawful access legislation in Canada, it was reported that 95 percent of requests for subscriber information by law enforcement officials were fulfilled voluntarily by the ISPs/TSPs inasmuch as these are already allowed (but not compelled) by law to divulge such information.[57] While this statistic has been used to question why the government needs to pass lawful access legislation, Canadians may want to consider whether this may be a problem in itself for their privacy. While not necessary by law for law-enforcement purposes, most often the license that customers sign with their ISP/TSP allows the company to share their information for law enforcement purposes.

As well, society has been quite liberal about the sharing of huge amounts of even intimate private personal information on social network services on the Internet. Most users of these services do not read the sweeping rights over their data that they sign (or, more precisely, "click") over to such companies as Google or Facebook. There also seems to be a great many individuals who reveal (in all senses of the term) personal details quite freely and publicly as content on social networking and dating websites.

We would suggest that libraries, whether public, school or academic, have a natural role in teaching citizens and students about web privacy matters as an aspect of information literacy. Even if libraries and library associations may not believe that they need to actively participate in a national debate specifically on new lawful access legislation, there is much positive and important work for them to do in order to educate their users on the privacy risks and issues that their users themselves will want to know about and consider acting upon. While education should be an unquestioned role for libraries and their associations, we would suggest that library associations, insofar as they may have the resources and freedom to do so, should also inform government of the general civil society concerns with issues such as lawful access that they may have: they are elements of civil society and libraries and their associations continue to have a moral authority that can be brought to bear on information policy issues, whether or not they directly affect libraries.

[57] Michael Geist, *Halifax Police on Refusals to Provide Subscriber Data: None* (19 March 2012), online: <http://www.michaelgeist.ca/content/view/6382/125/>.

Conclusion

The introduction of Bill C-30 has brought Canada closer to expanding the power of lawful access through the bill's permissible policing and surveillance activities, which raise important concerns for Canadian society at large or for Canadian libraries in particular, such as Internet privacy and intellectual freedom. If such legislation is passed, although unlikely for the current iteration of the bill, then Canadian libraries will draw upon experiences of nations that have already passed surveillance legislation into public law following 9/11, such as the United States and the United Kingdom. The library associations in these countries have played an important role in educating and raising awareness within their memberships of the potential for law enforcement agencies to seize or request information of a personal nature. In addition to briefing their members, library associations have also performed advocacy work at the national government level, and issued guidelines and policies that shape how libraries respond. As discussed, there is a decision to be made by associations as to how best to respond to lawful access legislation, especially in evaluating the specific risks it poses to the privacy of library users, whether as readers or as citizens. In the age of Facebook and Twitter, the notion of privacy is perhaps one that does not always resonate across all of today's population. However, it is an important right that is demanding of our attention, lest it be harmfully eroded.

About the Authors:

Brent Roe, MA, MLIS, Executive Director, Canadian Association of Research Libraries (Ottawa, Ontario, Canada), brent.roe@carl-abrc.ca

- Brent Roe has been Executive Director at the Canadian Association of Research Libraries since 2008, before which he was Associate University Librarian at York University in Toronto. His MA is in Ancient History and he has done reference and collection development in history as a librarian. He is a member of the Canadian Library Association Copyright Committee.

Jeannie Bail, JD, MSLIS, Information Services Librarian, Memorial University of Newfoundland (St. John's, Newfoundland and Labrador, Canada), jbail@mun.ca

- Jeannie Bail is an Information Services Librarian at the Queen Elizabeth II Library at Memorial University of Newfoundland. Before arriving at Memorial, she worked as Library Director at a private investment firm in New York, NY. She received her MSLIS from Pratt Institute and her JD from Brooklyn Law School. She is a member of the Canadian Library Association Copyright Committee.