


4-22-2015

What Next in a Post-C-51 Canada?

Mike Larsen

Kwantlen Polytechnic University

Follow this and additional works at: <http://kora.kpu.ca/facultypub>

 Part of the [Criminal Law Commons](#), [Criminology Commons](#), [Criminology and Criminal Justice Commons](#), [Law and Society Commons](#), and the [Public Policy Commons](#)

Original Publication Citation

Larsen, M. (2015). *What Next in a Post-C-51 Canada?* (CIIPS Research Report). Vancouver, B.C.: Canadian Institute for Information and Privacy Studies. Retrieved from <https://infoandprivacy.ca/wp-content/uploads/2015/07/Larsen-Research-Post-C-51-Canada.pdf>

This Report is brought to you for free and open access by the Faculty Scholarship at KORA: Kwantlen Open Resource Access. It has been accepted for inclusion in All Faculty Scholarship by an authorized administrator of KORA: Kwantlen Open Resource Access. For more information, please contact kora@kpu.ca.

What Next in a Post-C-51 Canada?¹

Mike Larsen, Kwantlen Polytechnic University

Several weeks before the 2015 Annual General Meeting of the Canadian Institute for Information and Privacy Studies, I spoke on a small panel alongside Professor Robert Diab² of Thompson Rivers University at an event entitled ‘Law, Rights, Security, and the New Anti-Terrorism Act’. The event took place at my own university, and for some of the students in the audience, it was their first real opportunity to learn about the contents and context of Bill C-51.³ As the event wrapped up, I invited attendees to contact me if they had any questions about my remarks or wished to continue to discuss the bill. One of the students who took me up on this offer posed a series of insightful questions about particular sections of C-51. She concluded her email with this question:

“One last thing. If I were to have protested or said anything against Bill C-51, and then later applied to work for the CBSA or RCMP, would that jeopardize my chances? (For instance, if I posted something on my social media accounts)”

This question is illustrative of the anxieties and uncertainties that characterize our present socio-historical context - the same anxieties and uncertainties that Bill C-51 emerges from, mobilizes, and amplifies. It was posed by a student seeking pragmatic guidance on how to make informed choices about the implications of political expression in a rapidly-changing surveillance society. It is also a clear example of the chilling effect of state surveillance;⁴ for every person who decides to pose such a question, how many simply opt to err on the side of caution and eschew political speech and activity so as not to create a career-limiting digital footprint? And, of course, there is much to be said about the implicit understanding of the nature and role of the state that

¹ These remarks are based on my address at the 2015 CIIPS AGM. The ideas and opinions expressed here are my own. I am grateful to the members of CIIPS for inviting me to share my thoughts with them, and even more grateful for the stimulating discussion that ensued.

² Robert Diab is the author of several publications on national security law in Canada, most recently *The Harbinger Theory*: Diab, R. (2015). *The harbinger theory: how the post-9/11 emergency became permanent and the case for reform*. Oxford, UK ; New York, NY: Oxford University Press. [<https://global.oup.com/academic/product/the-harbinger-theory-9780190243227?cc=ca&lang=en&>]

³ The openparliament.ca site for Bill C-51 provides the full text of the bill and an overview of its legislative history: [<https://openparliament.ca/bills/41-2/C-51/>].

⁴ Numerous groups, including the BCCLA, CJFE, and CAUT have spoken out about the potential chilling effects of Bill C-51. CAUT proposes that both the vagueness of C-51’s criminal code provisions regarding the advocating or promoting commission of terrorism offences and the expansive scope of the bill’s information sharing regime “will have a chilling effect on academic freedom and other forms of expression, advocacy, and protest”. [[http://www.caut.ca/docs/default-source/reports/bill-c-51-caut-analysis-\(2015-03\).pdf?sfvrsn=8](http://www.caut.ca/docs/default-source/reports/bill-c-51-caut-analysis-(2015-03).pdf?sfvrsn=8)]

informs the question. Tempting as it is to analyze the question, though, I am mindful that the student was hoping for a straightforward and helpful response.

So, how should we respond to such questions? I chose this opening vignette precisely because my honest answer at this point is *I don't really know*, and this seems like a good launching point for a discussion of the implications of C-51 and opportunities for research.

I don't really know, but I do know that political activity, including expression and activism that challenges government policy is and always has been a target of high policing in Canada.⁵ And I know that government guarantees that “lawful advocacy, protest, dissent and artistic expression” will not fall under C-51’s vast definition of “activity that undermines the security of Canada” are not reassuring. Community organizers and activists in Canada are no strangers to state surveillance. Recent examples include the infiltration of groups mobilizing against the 2010 G20 in Toronto, Ontario, and the monitoring of environmental activism in Canada.⁶ In both of these cases, stated concerns about the unlawful activities of a few served as pretext for extensive surveillance operations. Further, I know that applicants to police organizations are routinely asked about their Facebook pages, and that police recruiters advise those aspiring to careers in law enforcement to proactively police their own social media activity. So, while I cannot provide a straightforward ‘yes’ or ‘no’ answer to my student’s question, I can definitely say that the kinds of monitoring, political policing, and politicized recruitment that it contemplates are not unprecedented in Canada.

C-51 has now passed into law, and it will take some time for the full ramifications of the bill to become clear. It is an omnibus security bill consisting of five parts, several separate Acts, and a host of consequential amendments. It has codified an expansive definition of security, criminalized speech that supports terrorism offences, expanded the grounds for preventative arrest and detention, created a secretive framework for managing and renewing no-fly lists, further en-

⁵ For a detailed and authoritative history of political policing in Canada, see Whitaker, Kealey, and Parnaby’s book *Secret Service*: Whitaker, R. (2012). *Secret service: political policing in Canada: from the Fenians to fortress America*. Toronto: University of Toronto Press. Historian Steve Hewitt’s study of RCMP spying on Canadian university campuses is also informative: Hewitt, S. (2002). *Spying 101: the RCMP’s secret activities at Canadian universities, 1917-1997*. Toronto ; Buffalo: University of Toronto Press. Recent developments in the policing of dissent are discussed in the edited volume *Putting the State on Trial: The Policing of Protest During the G20 Summit*: Beare, M. E., Des Rosiers, N., & Dushman, A. C. (Eds.). (2015). *Putting the state on trial: the policing of protest during the G20 Summit*. Vancouver: UBC Press.

⁶ In February 2015, Desmog Canada publicized an internal RCMP “Critical Infrastructure Intelligence Assessment” report on “Criminal Threats to the Canadian Petroleum Industry”. The report, originally obtained by Greenpeace, offers a window into the RCMP’s monitoring of groups involved in protest and dissent related to the petroleum industry: [<http://www.desmog.ca/2015/02/17/leaked-internal-rcmp-document-names-anti-petroleum-extremists-threat-government-industry>]. Earlier reports on the surveillance of environmental groups and individuals involved in protests related to environmental issues led the BC-CLA to prepare a step-by-step Access to Information guide to assist requesters interested in gaining access to records about their activities held by the National Energy Board, RCMP, and other government institutions: [<https://bccla.org/dont-spy-on-me/10388-2/>]

trenched the security certificate mechanism, and expanded the ability of federal government bodies to engage in the warrantless sharing of personal information deemed relevant to national security (broadly understood). It has also - and perhaps most controversially - empowered the Canadian Security Intelligence Service (CSIS) to “take measures, within or outside Canada, to reduce” threats to the security of Canada. The practical scope of these powers is unknown, and it will likely fall to the courts to define their limits.⁷ I expect that in some cases, these challenges will only take place when an individual becomes aware of a perceived violation of his or her rights and initiates legal proceedings, and this is itself problematic given the secretive nature of some of the new powers created by C-51.⁸ Absent from the 60-page bill is any formal provision for expanded powers of investigation, oversight, or review for the patchwork of bodies responsible for national security accountability in Canada. The bill will have sweeping implications for privacy and information rights and civil liberties more generally.

Given the scope of the bill and the ambiguity of some of its provisions, I believe that it is uncontroversial to say that Canadian researchers working in the areas of surveillance and information and privacy studies have a lot of work ahead of us. Before we can come to terms with the long-term implications of the ‘post-C-51 context’, we will need to do some detail-oriented short-term and intermediate-term investigative work to get a sense of how the legislation is shaping everyday practice. What follows is a sketch of force connected information- and privacy-related research priorities that pertain to the implementation of C-51 over the coming months and years.

Four questions to inform a research agenda

Question 1: How are police and security personnel being briefed and trained regarding their post-C-51 mandates?

C-51 has expanded the mandates of numerous federal government organizations. CSIS has been provided with extensive ‘kinetic’ powers, and it will now be able to disrupt alleged threats to national security. Other C-51 provisions grant police expanded powers of preventive detention, empower both police and security services to seize online “terrorist propaganda” and criminalizes speech that “glorifies or promotes terrorism”.

⁷ As Reg Whitaker has pointed out, in an extraordinary inversion of the rule of law, C-51 makes it possible for CSIS to *break the law*, but prohibits the agency from *enforcing the law* (that being the province of peace officers). See Whitaker’s April 2, 2015 article in *The Tyee*, “Will Changes to C-51 Give Spy Agency Power to Detain?”: [<http://thetyee.ca/Opinion/2015/04/02/CSIS-C-51-Powers/>]

⁸ Professors Craig Forcese and Kent Roach have provided sustained and detailed analysis and commentary on the nature and implications of the various provisions of C-51. I recommend their June 9 article in *The Walrus*, “Why Can’t Canada Get National Security Law Right?”: [<http://thewalrus.ca/why-cant-canada-get-national-security-law-right/>]. See also their joint blog on C-51, *Canada’s Proposed Antiterrorism Act: An Assessment*: [<https://cdnantiterrorismmlawaudit.wordpress.com/about/>]. Forcese continues to write about the bill at his blog, nationalsecuritylaw.ca.

Now that C-51 has reached the implementation stage, it will be important to gather information about how the policing and security agencies most directly affected by the bill go about interpreting and exercising their new powers. Put differently, we need to begin to investigate C-51 from the bottom-up. Research questions abound, and include:

- How will the RCMP and CSIS go about interpreting the meaning and limits of the concept of “activity that undermines the security of Canada”? The term is found in the definitions section of the *Security of Canada Information Sharing Act*, but this definition is expansive and open to interpretation. Of particular interest will be the precise interpretation of what it means to interfere with “the economic or financial stability of Canada”.
- How will police and security personnel be trained to seek out and recognize “terrorist propaganda”? What roles will individual discretion and organizational policy play in this process? What kinds of resources will be allocated to investigations targeting terrorist propaganda?
- How will CSIS personnel be trained to exercise their new mandate for threat reduction? As a civilian intelligence service no longer composed primarily of former members of the disbanded RCMP Security Service, CSIS does not have a wealth of internal experience in ‘kinetic’ operations.⁹ Presumably, the expansion of its mandate under s. 42 of C-51 has led to considerable discussion about how CSIS personnel should go beyond intelligence collection, while stopping short of law enforcement.

Research regarding the activities of police and security agencies involved in the 2010 Toronto G20 Integrated Security Unit (ISU) illustrates the value of an approach that focuses on granular detail. For example, researchers using FOI requests obtained copies of slides and notes used at a pre-event training session for the Waterloo Regional Police Service. The slides offer an important window into the ‘middle ground’ between legislation and official policy and line-level practice. Crucially, they help us to understand how police commanders relayed the ‘mission’ and mandate of the G20 ISU to their subordinates, and how, through training, they constructed a particular set of expectations regarding the event.¹⁰ The departments and agencies most affected by C-51 will also be receiving briefings, directives, handbooks, and training sessions over the coming weeks and months. While it can be challenging for researchers to obtain such records, they offer invaluable insights. Research focusing on these sorts of materials is particularly important with regards to C-51, as it will help us to make sense of the impact of the bill in the interim period between its

⁹ The ‘civilianization’ of security intelligence in Canada was a response to the McDonald Commission’s inquiry into RCMP ‘dirty tricks’ in the 1970s. One of the key recommendations of McDonald’s report (and other reports the preceded it) was the separation of law enforcement and security intelligence powers and mandates. It is worth noting that many of the unlawful police operations that have come to be known as ‘dirty tricks’ - including mail openings, break-ins and data theft, sundry ‘countering’ activities intended to discredit perceived subversives, and the infamous burning of a barn - could now, following the passage of C-51, probably be carried out by CSIS personnel.

¹⁰ Independent journalist Tim Groves provides an excellent overview of the Waterloo Police training slides in his *Toronto Media Co-op* article “G20 police training exaggerated powers outside fence: files”: [<http://toronto.mediacoop.ca/fr/story/g20-police-training-exaggerated-powers-outside-fence-files/5470>]

implementation and the time that one or more of its provisions is first subject to scrutiny by the courts.

Question 2: What policies, procedures, and interpretations will govern the securitization and sharing of information within and between federal government institutions?

A major component of C-51 is the *Security of Canada Information Sharing Act*, s.5.(1) of which reads:

“Subject to any provision of any other Act of Parliament, or any regulation made under such an Act, that prohibits or restricts the disclosure of information, a Government of Canada institution may, on its own initiative or on request, disclose information to the head of a recipient Government of Canada institution whose title is listed in Schedule 3, or their delegate, if the information is relevant to the recipient institution’s jurisdiction or responsibilities under an Act of Parliament or another lawful authority in respect of activities that undermine the security of Canada, including in respect of their detection, identification, analysis, prevention, investigation or disruption”.

Schedule 3 lists a number of Government of Canada bodies, including the ‘usual suspects’ involved in national security - for example, CSIS, the RCMP, and the CBSA - as well as organizations like the Canada Revenue Agency, Department of Finance, and Department of Health. The institutions in receipt of information disclosed under s. 5.(1) may further use and share the information, and, under s.10.(1) of the Act, the Minister of Public Safety and Emergency Preparedness may recommend to the Governor in Council regulations respecting the manner in which records shared under s.5. are disclosed and retained.

In practical terms, this *Act* has expanded the capability of Government of Canada bodies to engage in the sharing of personal information. It has also extended the already-big tent of the security field by explicitly providing the Department of Health and CRA with national security mandates. Note that the institutions listed in the schedule (which itself may be amended) are designated *recipient* institutions. Any Government of Canada body may act as a *disclosing* institution, either on its own initiative or upon request.

How exactly will this system of disclosure and receipt operate? In order for the *Security of Canada Information Sharing Act* to function, government bodies will have to interpret what constitutes information that might relate to “activities that undermine the security of Canada”. The definition of this concept provided by C-51 is expansive, and it essentially creates a mandate for Government of Canada employees to adopt an “if you see something, say something” mentality with respect to information under their control. Under the *Act*, an employee of Heritage Canada, the Department of Fisheries and Oceans, or Aboriginal and Northern Affairs Canada (or any other Government of Canada institution) has the potential to initiate a process of disclosure provided that he or she perceives the information in question to be relevant to the jurisdiction of any of the scheduled recipient institutions in relation to “activities that undermine the security of Canada”. This initiation of disclosure would take place outside of any warrant system or other

court proceeding. Of immediate interest to me is how various government institutions whose mandates do not typically focus on national security will brief and train their employees regarding what constitutes suspicious information and how to proceed if they come across it. This process of briefing and training should create a paper trail that will be accessible to researchers under the Access to Information Act (ATIA). Access requests for briefing notes, policies and procedures, memorandums, and training materials (slides and decks) may help to shed light on the ‘whole of government’ impact of the *Security of Canada Information Sharing Act*.¹¹

I doubt that most information sharing arrangements under s.5. of the *Act* will take such an unorganized, bottom-up form, though. It is far more likely that recipient institutions listed in Schedule 3 of the *Act* will initiate relationships with various government bodies regarding the disclosure - upon request or on an ongoing basis - of certain types of information. Such arrangements may be governed by the regulations set out in s.10.(1) of the *Act*, or they may take the form of Letters of Understanding or Memorandums of Understanding between government bodies. These too should be sought by researchers through ATI requests. It will be particularly important to obtain records that explain how personal information (as defined by the *Privacy Act*) disclosed pursuant to s.5. will be used, shared, and retained by government agencies.

Question 3: How will the C-51 changes impact intergovernmental collaboration and information sharing, especially with respect to personal information?

C-51 applies primarily to federal institutions, including the RCMP, CSIS, and other Government of Canada bodies involved in ‘security work’ (broadly defined). The new *Criminal Code* provisions are technically enforceable by police operating at any level, but I expect that the RCMP will take the lead in investigations regarding “terrorist propaganda” and in the use of preventative detention. Much of the debate regarding C-51 has, understandably, focused on its implications for the activities of federal government institutions.

It is important to bear in mind, however, that investigative and enforcement activities associated with ‘national security’ are not the sole province of federal departments and agencies. The contemporary security field is characterized by integration and collaboration - between agencies, between levels of government, between public and private sectors, and across national boundaries. Consider the unprecedented experiment in multi-agency collaboration that was the 2010 G8-G20 Integrated Security Unit (ISU). This involved the coordination of federal, provincial, and municipal policing and security organizations as well as private security contractors. One component of this massive undertaking was the use of an integrated Joint Intelligence Group, or

¹¹ Researchers interested in taking up this investigative work may find it helpful to refer to *Access in the Academy: Bringing ATI and FOI to Academic Research*, a guidebook I prepared for the BC Freedom of Information and Privacy Association: [<https://fipa.bc.ca/wordpress/wp-content/uploads/2014/06/Access-in-the-Academy.pdf>]. For additional analysis and commentary on research using ATI/FOI mechanisms, see the edited volume *Brokering Access: Larsen, M., & Walby, K. (Eds.). (2012). Brokering access: power, politics, and freedom of information process in Canada*. Vancouver: UBC Press: [http://www.ubcpress.ca/search/title_book.asp?BookID=299173819]

JIG. The following brief description of the activities of the JIG is from the RCMP's own post-event After-Action Report:

The Summits JIG was established in December 2008. Its mandate was to collect and disseminate information and intelligence in a timely manner to assist in the decision making process in both planning and implementation phases of the Summits.

The JIG comprised approximately 500 personnel from key stakeholders such as the RCMP, OPP, TPS and Peel Regional Police, CSIS, CBSA, the CAF and Transport Canada. The JIG identified criminal activity and other threats to the Summits and relayed those risks to the appropriate partners. Threats were detected and communicated to decision makers in a timely manner.¹²

The G20 JIG stands out because of its scale, but not because of its form; temporary and standing collaborative arrangements are a feature of contemporary policing and security work.

What does this have to do with C-51? The *Security of Canada Information Sharing Act*, as discussed earlier, enables a greatly-expanded system of information-sharing between institutions within the Government of Canada - and many of these institutions are already parties to information-sharing arrangements with provincial and municipal government bodies. It is reasonable to expect that federal government institutions will receive, from municipal or provincial partners, information - including personal information - that meets their working definition of information respecting "activities that undermine the security of Canada", per s.5(1) of the *Act*. The federal government institutions in question would then be in a position to disclose relevant information to the designated "recipient institutions", either voluntarily or in response to a request. Indeed, in a security context characterized by INSETs, joint task forces, and JIGs, this seems inevitable.

This, I propose, has real implications for the municipal and provincial government bodies involved in such collaborations. Once information that may have some perceived link to "activities that undermine the security of Canada" is received by an institution that is part of the Government of Canada, that information may be shared (and re-shared) within and between the various agencies that now have a defined national security mandate. Will municipal and provincial government bodies - for example, police services - be able to guarantee that they are sharing information with federal government partners in a way that is compliant with provincial Freedom of

¹² See "Finding 4: Collection and dissemination of intelligence through one central team supported the partners in working together", from the *RCMP 2010 G8 and G20 Summits RCMP led Horizontal Evaluation Report*: [<http://www.rcmp-grc.gc.ca/aud-ver/reports-rapports/G8-G20-eng.htm#Findings>]. For a detailed discussion of networked security and intelligence activities during the G20, see Beare, M. E., Des Rosiers, N., & Deshman, A. C. (Eds.). (2015). *Putting the state on trial: the policing of protest during the G20 Summit*. Vancouver: UBC Press.

Information and Privacy laws?¹³ In a post-C51 context, it may be difficult to predict the post-disclosure destiny of such information with any real confidence. This should give provincial and municipal agencies reason to reconsider the nature and extent of their information-sharing arrangements with federal partners. Provincial and territorial Information and Privacy Commissioners may also wish to examine these arrangements to ensure that government bodies under their jurisdiction are able to meet their obligations with respect to the treatment of personal information under their control.

For researchers working in the information and privacy field, there is a need - and an opportunity - to investigate the 'trickle-down' implications of C-51 at the sub-federal levels.

Question 4: How will the C-51 changes impact information and privacy rights under the *Access to Information Act* (ATIA) and *Privacy Act*?

Despite its many shortcomings, I have found the ATIA to be a powerful - if inconsistent - tool for conducting research on the organizations and practices that characterize the Canadian national security field.¹⁴ C-51 has the potential to exacerbate a number of already-existing problems encountered by requesters working in the area of national security and by individuals seeking access to personal records that might relate to national security investigations. Two specific challenges come to mind.

The first potential challenge relates to the "law enforcement and investigation" exemptions found in s. 16 of the ATIA and s. 22 of the *Privacy Act*. Section 16.(1) of the ATIA allows the head of a government institution in receipt of an ATI request to refuse to disclose any record that contains *inter alia*, information pertaining to "activities suspected of constituting threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act*".¹⁵ Similarly, section 22.(1) of the *Privacy Act* allows the head of an institution in receipt of a request to refuse to disclose personal information "that was obtained or prepared by any government institution, or

¹³ During the May 11 session of Parliament, NDP MP Dan Harris posed a question about whether information contained in the Toronto Police 'carding' database could be subject to access or sharing under the provisions of the *Security of Canada Information Sharing Act* [<https://openparliament.ca/debates/2015/5/11/dan-harris-1/>]. While the *Act* does not give federal policing and security agencies a new right of access to records maintained by municipal or provincial government bodies, if such records were shared in the context of a collaborative security arrangement (for example, a JIG), they could be subject to the disclosure and sharing provisions of C-51.

¹⁴ See, for example: Larsen, M. (2014). Indefinitely Pending: Security Certificates and Permanent Temporariness. In V. Preston, L. F. Vosko, & R. Latham (Eds.), *Liberating Temporariness?: Migration, Work, and Citizenship in an age of Insecurity* (pp. 76–96). Montreal & Kingston: McGill-Queen's University Press.

¹⁵ Access to Information Act (R.S.C., 1985, c. A-1) [<http://laws-lois.justice.gc.ca/eng/acts/a-1/FullText.html>]. Note that the definition of "threats to the security of Canada" under the *CSIS Act* overlaps partially - but not entirely - with the definition of "activity that undermines the security of Canada" under C-51. The *CSIS Act* definition is comparatively narrow.

part of any government institution, that is an investigative body specified in the regulations in the course of lawful investigations pertaining to [...] activities suspected of constituting threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act*".¹⁶

It will be interesting to see whether how and these clauses will be applied to exempt from disclosure information that has been shared between institutions under the *Security of Canada Information Sharing Act*. Consider a hypothetical scenario: The Department of Health discloses a mix of personal information and general government records to CSIS pursuant to s. 5.(1) of the *Act*. Subsequently, the Department of Health receives requests for some of this information under the ATIA and *Privacy Act*. Will the Department of Health ATIP Unit take the position that, by virtue of their being disclosed under s. 5(1), the records in question are presumed to pertain to "activity that undermines the security of Canada", and that they are, by extension, subject to exemption under the applicable "law enforcement and investigation" clauses? Would the scenario be different if the Department of Health had disclosed the records in question to the Department of Public Safety and Emergency Preparedness (or another institution) as opposed to CSIS? Would the outcome be different depending on whether the information was volunteered or requested by the recipient institution?

To reframe the question in general terms: Will the mere fact that information has been subject to disclosure under s.5(1) of the Security of Canada Information Sharing Act be presumed to exempt it from disclosure under the ATIA or *Privacy Act*?

The second challenge relates to the structural mismatch between the federal ATI process and the nature of work in the security field. Put simply, the ATIA works best when access requests focus on information contained in the records of individual government institutions. A product of the bureaucratic culture of the early 1980s, the *Act* seems to reflect a vision of government characterized by neat jurisdictions and information 'stovepipes'. However, contemporary national security practices, as mentioned earlier, are increasingly collaborative in nature, characterized both by flows of information within institutions and by flows of information between institutions. In my experience, this means that requests under the ATIA are often subject to lengthy extensions under s. 9.(1)(a) and (b), which state that:

9. (1) The head of a government institution may extend the time limit set out in section 7 or subsection 8(1) in respect of a request under this Act for a reasonable period of time, having regard to the circumstances, if

(a) the request is for a large number of records or necessitates a search through a large number of records and meeting the original time limit would unreasonably interfere with the operations of the government institution,

¹⁶ Privacy Act (R.S.C., 1985, c. P-21) [<http://laws-lois.justice.gc.ca/eng/acts/P-21/FullText.html>]

(b) consultations are necessary to comply with the request that cannot reasonably be completed within the original time limit,¹⁷

The consultations mentioned in s. 9.(1)(b) can take place when the government body in receipt of an ATI request deems it necessary to seek the opinion of other government bodies with some involvement in the information in question prior to releasing records. This contributes to lengthy extensions (often 120 days or more), and to a general delay in the ATI process.¹⁸ By expanding the scope of information-sharing between departments and agencies, Bill C-51 may further increase the likelihood that ATI requests pertaining to security issues will be subject to consultation-related extensions. Whether and to what extent my concern about this is on-point will become apparent over the next year, as security-related ATI requests (especially those pertaining to C-51 topics) work their way through the system.

Conclusion:

This overview of post-C-51 research priorities is, of course, non-exhaustive. There are so many outstanding questions regarding the bill that it can feel difficult to know where to begin. This suggests the need for cooperation and partnerships - between researchers, community-based organizations, and other bodies interested in contributing to a sustained dialogue about this latest chapter in Canadian (in)security. I think that CIIPS has a vital role to play in this process.

¹⁷ Access to Information Act (R.S.C., 1985, c. A-1) [<http://laws-lois.justice.gc.ca/eng/acts/a-1/FullText.html>]

¹⁸ For commentary on this, see: Walby, K., & Larsen, M. (2011). Getting at the Live Archive: On Access to Information Research in Canada. *Canadian Journal of Law and Society*, 26(03), 623–633.