THE EFFECTIVENESS AND ACCOUNTABILITY OF CANADA'S INTELLIGENCE AGENCIES: VIEWS FROM PARLIAMENT

By: Iván A. Narváez

Iván Narváez is a graduate of the Norman Paterson School of International Affairs and recently completed ten months on Parliament Hill as part of the non-partisan Parliamentary Internship Program, working for James Bezan, Parliamentary Secretary to the Minister of National Defence, and Liberal Foreign Affairs Critic Marc Garneau.

Introduction

The 41st Parliament has witnessed an uncommon amount of attention being paid to intelligence and national security issues. This is thanks in no small part to the steady trickle of leaked documents coming from former National Security Agency (NSA) contractor Edward Snowden, via journalist Glenn Greenwald. At the end of January 2014, leaked documents suggested the Communications Security Establishment Canada (CSEC) may have engaged in some form of metadata collection program at a Canadian airport, *prima facie* in violation of its legal mandate not to target Canadians or individuals in Canada.[1] In response, both the House of Commons Standing Committee on National Defence and the Senate Standing Committee on National Security and Defence held hearings with the Chief of CSEC, among others, to discuss the metadata collection activities of this agency and the accountability of Canada's intelligence agencies more broadly.[2]

This Parliament also saw the launching of a lawsuit by the British Columbia Civil Liberties Association (BCCLA); the moving of motion M-461 to, among other things, study the appropriate methods of parliamentary oversight of Canadian intelligence policies and agencies, by New Democratic Party (NDP) National Defence Critic Jack Harris; the introduction of the *National Security Committee of Parliamentarians Act* (C-551) by Liberal Public Safety Critic Wayne Easter; the *CSEC Accountability and Transparency Act* (C-622) by Liberal National Defence Critic Joyce Murray; and the introduction of the *Intelligence and Security Committee of Parliament Act* (S-220) by Conservative Senator Hugh Segal.

Unlike the debate that emerged in response to the terrorist attacks of September 11, 2001 which understandably focused on the effectiveness of Canada's intelligence enterprise, this debate has focused more on the accountability of intelligence agencies.

Methodology

The intent of this study is to explore the views of Members of Parliaments (MPs) on how effective and accountable Canada's intelligence agencies are. It is an entirely qualitative study (despite the use of a survey), and its value to policymakers, practitioners, and academics is to be found in providing a snapshot of concerns MPs may have with respect to these themes, and their amenability to various proposed reforms to address their concerns.

Scope

To set the parameters of this study, when referring to intelligence agencies the MPs were prompted that the agencies specifically being referred to were the Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment Canada (CSEC). While there are certainly more agencies and departments involved in the Government of Canada's intelligence community,[3] these two were chosen in particular as they are both civilian agencies, dedicated solely to intelligence gathering, and are most intimately involved with national security issues. While a useful debate could certainly be had about the effectiveness and accountability of the national security intelligence gathering activities of the Royal Canadian Mounted Police (RCMP) or the Canadian Armed Forces (CAF), to name just two, in consideration of the limited time MPs can devote to an academic study above and beyond their regular duties, the study has attempted to maintain as narrow a scope as possible on what agencies would uncontroversially be considered intelligence and national security related.

Data collection

The first stage of data collection was conducted through the use of an anonymous online survey, active from the end of May through June 2014. The survey contained nine substantive questions, in addition to standard biographical questions, and was circulated in both English and French. The survey was designed to be short to maximize the response rate and, as mentioned above, its purpose was to narrow in on the issues that were top of mind for MPs so that they could be explored in greater depth in follow-up interviews.

The result of this survey was only a moderate success. While only seven MPs completed the survey, it is notable that all officially recognized parties were represented. Respondents also included both genders; younger and older MPs; first term MPs and MPs with over a decade in the House; Westerners, Ontarians, Quebecois, and Maritimers; rural, urban, and suburban constituencies; members of relevant committees; and Members with previous professional experience in the military or law enforcement. Despite the relatively small number of respondents, the results are fortunate to be based on a diverse set of MPs, particularly in terms of party representation and MPs with varying levels of familiarity with the issue area.

The second stage of data collection was a series of targeted interviews that built on the results of the survey. In total, four of these supplementary interviews were completed. They all took place in mid-June 2014. The interview requests were targeted at MPs with a specific interest in national security issues, as determined by their assigned portfolios and committee membership. Once again, representatives of all parties were interviewed. The four interviewees were: Rick Norlock (Conservative Party of Canada), Chair of the National Defence Committee and member of the Public Safety Committee; James Bezan (Conservative Party of Canada), Parliamentary Secretary to the Minister of National Defence; Jack Harris (New Democratic Party), National Defence Critic; and, Wayne Easter (Liberal Party of Canada), Public Safety Critic.

Interviews varied in length from 15 minutes to an hour, depending on the availability of the MP. As mentioned above, the interview questions largely built on the results of the survey and did not repeat questions. As the survey was anonymous, it is unknown if any MPs participated in both the survey and interview portions of the study. All interviews were "on the record", but were not recorded or transcribed. All references to what MPs said in the interviews are based on notes taken by the author and are not direct quotations. They are therefore dependent on the author's subjective interpretation of the comments in the context in which they were made.

Summary

In sum, the study reflected below is a qualitative, exploratory endeavour. Based on the views of nearly a dozen MPs, it examines two critical themes in the realm of intelligence policy making: effectiveness and accountability. It aims to provide three things: a snapshot of the views of MPs at a point in time when intelligence and national security issues have been receiving an unusual amount of political and public attention, the amenability of MPs towards various existing proposals for reform of Canada's intelligence agencies, and to generate questions for future research.

Effectiveness

The first theme of the study, effectiveness, is centred around the broad question of "Are these agencies doing their job?" One might similarly ask if they have the right powers and the right priorities. The national security threats currently facing Canada are diverse. CSIS Director Michel Coulombe writes that terrorism remains the foremost concern of CSIS.[4] Also highlighted are espionage and cybersecurity, with the CSIS website listing the proliferation of weapons of mass destruction (WMDs) as an additional priority. Coulombe states we live in a world where the methods by which Canadian interests can be harmed are expanding.[5] Similarly, the "Strategic Environment" section of the Government's *Canada First Defence Strategy* states "Canadians live in a world characterized by volatility and unpredictability."[6]

Indeed, some scholars speak of a paradigm shift since the terrorist attacks of 9/11, to a conceptualization of national security more focused on non-state actors than state actors, which undoubtedly increases the number and diversity of threats facing a state.[7] The Conference of Defence Associations Institute (CDAI), a non-partisan think tank focusing on national security and defence issues, outlines a variety of risks and threats to Canada in its 2014 Strategic Outlook. A non-exhaustive list includes "China's long-term ambitions and the future of a multipolar world", crises in Syria, Libya, and Iraq, and cybersecurity.[8] The authors of this report state, "... there is no shortage of crises and the international environment is less secure today than it has ever been[.]"[9]

Results

It is in this context that this study queried the opinions, priorities, and concerns of MPs regarding the effectiveness of Canada's intelligence agencies. At the highest level, all MPs who participated in the study expressed confidence in the effectiveness of Canada's intelligence agencies. In the survey portion, four MPs indicated they felt Canada's intelligence agencies were 'somewhat effective' and three indicated 'effective' (ratings of '5' and '6' out of a 7 point scale respectively).

Regarding the priorities of intelligence agencies, MPs were asked to rate a series of possible priorities on a scale of 1 to 7, with 1 being 'not at all important' and 7 being 'very important'. The order in which the priorities were presented to MPs was randomized for each respondent, and the results presented here are an aggregation of both the French and English surveys (as is the case in all figures presented throughout the paper). Top priorities in MPs' minds were largely aligned with the existing priorities of intelligence agencies, namely counter-terrorism, cybersecurity, and counter-espionage. Certain countries were also included in the list, with Russia and China coming out as top concerns.

Lastly, MPs were surveyed about various existing proposed policy and/or institutional changes that might affect the effectiveness of Canada's intelligence agencies. Similar to how the question on priorities was conducted, MPs were asked to rate on a scale of 1 to 7 their level of agreement with a given proposal. Once again, the order in which proposals were presented was randomized for each respondent. In this case, no proposals gained clear support from MPs. The single appearance of consensus emerged in that MPs were unanimous in their opinion that Canada should not engage in industrial espionage. Otherwise, all other proposals, such as the creation of a foreign human intelligence gathering agency or the suggestion that existing agencies should receive increased resources, received mixed reviews.

Analysis: Challenges of cybersecurity

While the survey portion of the effectiveness theme did not seem to provide particularly unique or notable results, the follow-up interviews produced an interesting finding in the realm of cybersecurity. Wayne Easter, the first MP to be interviewed, expressed his concern about the vulnerabilities created by our society's increasing dependence on the internet, saying he feared that the next 9/11 would be an electronic attack. Similarly, Rick Norlock expressed the thought that the cyber-realm was the “direction terrorism is going in all the western world”, while also noting the advanced capabilities being developed by state actors.

While these concerns around cybersecurity may be linked to the active Parliamentary debates around the activities of CSEC, it is also true that cybersecurity and the implications of technological change have been receiving a great deal of attention from academics, the policy community, and other experts as of late. For example, Clarke and Knake's 2010 book “Cyber War” provides a highly readable analysis of the threat posed by state actors. Beyond capabilities that could hypothetically be developed, they point to already existing examples that demonstrate the seriousness of cyber-weapons. The most famous (and sophisticated) example is likely the *Stuxnet* virus that appears to have targeted Iranian nuclear facilities.[10] The authors believe that the US and possibly Israel were behind this attack (and media reports later appear to have confirmed this).[11]

As for the other major state powers, Russia has been strongly implicated in cyberattacks on its neighbours, including during its invasion of Georgia in 2008 and during a dispute with Estonia[12], and Chinese military leaders have published books on how to leverage their cyber-capabilities (among other tactics) in a conflict with the US.[13] Castaldo quotes General Keith Alexander, former head of the United States Cyber Command as saying, “The platform we have today is not defensible. I would guarantee you that the adversary could penetrate it, and it'd take us months to find it.”[14] Certainly it stands to reason then that if the world's only superpower is not prepared for cyber attacks, surely Canada has something to be worried about too.

In a more Canada-specific analysis, Gendron examines the “multiplier effects” of cyber threats – that is, how reliance on the cyber-realm has “imbued traditional threats with new life” by either magnifying their potential impact and/or increasing their likelihood.[15] She notes that as Canadian society becomes increasingly dependent on information and communications technologies, we become increasingly vulnerable to a growing diversity of cyber threats.[16] Critical national infrastructures (CNI) society depends on, on a daily basis, are, to varying degrees, dependent on or vulnerable to the cyber-realm.[17]

Lastly, there is the analysis of the Government of Canada's cybersecurity situation offered by John Adams, former Chief of CSEC. Adams conceives of cyberspace as a fourth global commons (along with the sea, air, and space). To assure national security, let alone thrive as a nation, he argues a state must have some ability to navigate these commons.[18] Notably, Canada is one of the most wired nations on earth, ranking first in amount of time spent online, and conducting a significant amount of online shopping, banking, communication, and entertainment activities, to name just a few.[19] That said, Adams also notes the pressure to innovate and/or provide greater convenience has meant that changes in functionality outpace adequate adaptations in security.[20]

Rightfully then, it would appear MPs are correct to be concerned about Canada's cybersecurity – and this discussion has focused only on the national security dimensions. Unfortunately, there appears to be a dearth of innovative solutions in the minds of MPs to address this challenge, and there is mixed support at best for increasing the budgets or powers of existing agencies. As Rick Norlock stated, the country could “go broke” trying to keep up with the ever-changing cyber landscape.

Accountability

The second theme of this study, accountability, examines the mechanisms that review and oversee the activities of Canada's intelligence agencies. First, while the terms 'review' and 'oversight' might on the surface appear to be synonyms to some, the terms are used for distinct purposes in this study. As Shore defines them, 'review' is the audit of past actions or policies while 'oversight' is the exercise of on-going control over the policies, procedures, and activities of agencies.[21] In combination, they feed into what this study terms 'accountability'.

In Canada, a variety of mechanisms and organizations exist to review and oversee intelligence agencies. Most prominently, the Security Intelligence Review Committee (SIRC) acts as an independent review body that reports to Parliament on the activities of CSIS, as well as investigating public complaints made about CSIS.[22] SIRC is independent of CSIS and reports directly to Parliament by providing an annual report (that is also released publicly) detailing every study, query, and complaint investigated.[23] Also notable, it has recently absorbed the functions that the Inspector General of CSIS used to perform.[24] Correspondingly, the Office of the Communications Security Establishment Commissioner performs a similar role to SIRC, in relation to CSEC. Differently however, the Commissioner reports to the Minister of National Defence, who then tables reports to Parliament.[25]

These bodies are not the only ones charged with the accountability of Canada's intelligence agencies however. Of course, at the highest level, Ministers of Public Safety and National Defence retain overall responsibility for the actions of CSIS and CSEC respectively. The Ministers and agencies are also responsible to their respective Parliamentary committees for general policy direction and, as seen recently with the Snowden leaks, when a crisis emerges.[26] Intelligence agencies, like all other departments and agencies of government, are also held to account in more specific fields by various agents of Parliament, such as the Auditor General, the Privacy Commissioner, and others. They are furthermore bound by the laws of the land and the court system that upholds them, including the CSIS Act, the National Defence Act, the Privacy Act, the Access to Information Act, the Charter of Rights and Freedoms, the Criminal Code, among others.[27]

As Canada's intelligence agencies are given exceptional powers to encroach upon the privacy of citizens, so too has Parliament built various institutions to ensure the appropriate behaviour of these organizations. The views of experts on the accountability of Canada's intelligence agencies has, in recent months at least, been mixed. On the positive side, some have pointed to the helpful role of independent, expert review bodies such as SIRC providing a service that Parliamentarians would be hard-pressed to do themselves.[28] Similarly, Penney notes most commentators have concluded SIRC is effective in holding CSIS accountable, and that the combination of SIRC review and the judicial warrant process CSIS goes through to conduct investigations serves as a sufficient guard against undue intrusions on privacy.[29]

However, certain gaps and deficiencies have also been identified. Bailey argues Canada is at a crossroads in terms of systematic access to information held in the private sector by the government. She notes that while prior judicial authorization for the collection of private data has been the practice, this is now being challenged by CSEC's ability to conduct surveillance of Canadians with only Ministerial approval, compulsion of private organizations to disclose personal information to authorities, and provisions that allow for easier or warrantless access to data.[30] Penney argues that the authority of the RCMP to conduct communications surveillance in terrorism investigations without establishing investigative necessity and allowing CSEC to intercept domestic communications without prior judicial authorization are “constitutional infirmities” that should be found in violation of section 8 of the Charter.[31] Many other criticisms have been levelled against the government's surveillance activities of late, particularly with regard to CSEC's metadata collection program. As they are particularly relevant to the findings of the survey and interviews, they will be treated in greater detail below.

Results

In contrast with the high-level findings under the effectiveness theme, MPs were less certain Canada's intelligence agencies are accountable. Of the seven surveyed, two felt Canada's intelligence agencies are 'not accountable' or 'somewhat not accountable', and another two were neutral to the proposition. Also contrasting with the first theme of the study, there was much more unanimity in attitudes towards proposed reforms to improve accountability. MPs expressed nearly undivided support for reforms to the legislation governing intelligence agencies, Minister's enacting changes already within their power, and Parliament taking an increased role in the oversight of intelligence agencies.

Unsurprisingly, concerns around the collection of metadata were very much present in the minds of MPs. Only one MP reported the sentiment that metadata did not contain or represent sensitive personal information (and one was neutral). In an open comment question, one MP wrote, "The collection of metadata is of profound concern. We need to ensure that privacy is not sacrificed to paranoia. There needs to be careful oversight."

The targeted interviews provided a wealth of additional information. Looking at their preferred methods of increasing accountability, there is a tendency to favour the United Kingdom's model of a committee of parliamentarians overseeing all intelligence services. Rick Norlock and Wayne Easter expressed general support for this model, and Hugh Segal's bill creates a committee that appears to be modelled after the UK system. Jack Harris, while not committing to support a particular model of parliamentary oversight, was clear in his support for a strong role for parliamentarians in general in the process. Taking a somewhat sceptical view however was James Bezan, who noted that this type of committee oversight structure would require MPs to set aside partisan differences as well as to take an oath of secrecy; something he felt not all MPs would be prepared to do, citing the NDP's refusal to participate in the committee of parliamentarians that studied the Afghan detainee files. That said, the fact remains the UK model of parliamentary oversight was the most cited and most supported among the MPs interviewed, and these views are notable in crossing party lines.

Analysis: Privacy and metadata

In the political context of the 41st Parliament, it is unsurprising that accountability and concerns around metadata seem to have been of greater concern to MPs than the effectiveness of intelligence agencies. Public opinion polling found only 8% of Canadians trust their personal information in CSEC's hands.[32]

Parliamentarians quickly caught on to these shifting winds, as evidenced by the three bills related to intelligence oversight introduced in this session along with a motion to study the appropriate methods of parliamentary oversight of Canadian intelligence policies and agencies. Parliamentary committees in the House of Commons and the Senate also held a series of hearings exploring the intelligence gathering practices of CSEC, featuring the Minister of National Defence and the Chief of CSEC.[33] Clearly, these issues were a significant concern to Parliamentarians. The question then becomes: to what extent did they have reason to be concerned?

First, it is important to clarify what precisely metadata is. The Information and Privacy Commissioner of Ontario defines metadata as "information generated by our communications devices and our communications service providers, as we use technologies like landline telephones, mobile phones, desktop computers, laptops, tablets or other computing devices."[34] While metadata does not include the specific content of communications made through these devices, it does include "information that reveals the time and duration of a communication, the particular devices, addresses, or numbers contacted, which kinds of communications services we use, and at what geolocations."[35]

Expert opinion on how sensitive this information can be is split. On one hand, some point to the ability of analysts to use metadata to construct a portrait of an individual's relationships, affiliations, patterns of travel, and even sleep habits, among many other details.[36] On the other hand, others have called the recent debate disingenuous and unsophisticated in light of the widespread investments private companies are making into advanced customer tracking and analytical tools, with little to no outcry.[37]

Perhaps most significantly, recent legal analyses have raised concerns over parts of CSEC's metadata collection program and the authorities used to conduct it. Forcese finds that because some metadata could fit the legal definition of a "private communication", ministerial authorization should always be sought by CSEC when metadata is being collected, and that a judicial warrant process (along the lines of what CSIS already does) should be added when the privacy of Canadians can reasonably be expected to be affected by surveillance activities.[38] Similarly, Penney finds that the domestic surveillance powers given to CSEC by the Anti-Terrorism Act would likely fail a section 8 Charter challenge, while at the same time noting that the search and surveillance powers set out in the CSIS Act strike a reasonable balance between the competing interests of national security and privacy.[39] From this preliminary analysis, it appears the expert community would tend to favour relatively straightforward reforms, in the sense they can be modelled on the existing accountability structures for CSIS.

This contrasts interestingly with the stated desire of some MPs for a greater role in oversight of intelligence agencies, and the various bills addressing this issue currently before Parliament. As noted in the preceding section, there is an interest among MPs in pursuing an accountability model similar to that of the UK. A variety of reasons were put forward to support a greater role for parliamentarians, including depoliticizing intelligence issues and the desirability of vigorous debate.[40] Expert commentators however have been more sceptical about the utility of greater involvement of parliamentarians. Shore notes duplication of efforts, security of information, lack of expertise, and general unreliability due to changes in membership and electoral cycles as reasons a parliamentary committee would not be well suited to a review and/or oversight function.[41] It would seem then that further study of the ideal means of ensuring the accountability of intelligence agencies would be beneficial, and that experts might find receptive audiences for their input on Parliament Hill as these bills go forward.

Conclusion

In closing, this study has aimed to explore the views and attitudes of parliamentarians regarding current issues facing Canada's intelligence agencies. Generally speaking, it would appear MPs with particular knowledge of this issue area are preoccupied by the challenge of cybersecurity. Relatedly, a wide range of MPs appear to be concerned about the accountability of Canada's intelligence agencies, particularly as it pertains to electronic eavesdropping.

As this is a qualitative study based on a limited sampling of MPs, conclusions derived from the research can only be tentative. They do, however, provide starting points for future studies that may go into greater depth. While it was not foreseen at the outset of the study, a unifying theme in the form of cybersecurity and privacy emerged that linked the pillars of effectiveness and accountability together. A review of some of the implications of developments in the cyber realm has been provided in this paper, but due to the scope of this study, a complete picture is better left to future research.

As Wayne Easter noted during his interview, forward-looking intelligence policy faces a bit of a paradox in that cybersecurity presents one of, if not the, most significant challenges to Canada's national security, while at the same time technological developments pose the most serious risk to Canadians' privacy. Of course, these need not be mutually exclusive outcomes. Clearly, there is a need for policy-makers to face these challenges sooner rather than later. It is interesting to read the Proceedings of the Intelligence Review Agencies Conference, hosted by SIRC in Ottawa in 1999, titled "Review and Oversight in the New Millennium: Challenges of a Multiploar World." A remarkable number of challenges noted in 1999 remain relevant today, including the role of parliamentarians in review and oversight, public scepticism about the activities of intelligence agencies, and getting the balance between privacy and national security right.[42] Tasseron notes the generational quality to these debates that parallel other advancements in technology, from satellites in the 1970s to the proliferation of video cameras in the 1990s.[43] He concludes by arguing urgently for a practical and sophisticated debate on how best to adapt oversight and legal frameworks to disruptive technological innovations, as they cannot be undone.[44]

In the end, future studies could prioritize some of the preliminary findings of this paper. In terms of the effectiveness theme, MPs could be probed further as to how great a threat they perceive cybersecurity to be, and particularly how they feel it compares to other threats such as terrorism. As for the accountability theme, it would be interesting to re-examine MPs concerns with metadata at a later date to determine how much concern is driven by the current attention to this issue. It will also be interesting to see what, if any, reforms are made to the review or oversight bodies of Canada's intelligence agencies as a result.

Endnotes:

[1] Craig Forcese, "Law, Logarithms and Liberties: Legal Issues Arising from CSEC's Metadata Program," *March 2014 SSRN Draft* (2014): 1.

[2] See: http://www.parl.gc.ca/CommitteeBusiness/CommitteeHome.aspx?Cmte=NDDN&Language=E&Mode=1&Parl=41&Ses=2 for the House Standing Committee, and http://www.parl.gc.ca/SenCommitteeBusiness/CommitteeHome.aspx?parl=41&ses=2&Language=E&comm_id=76 for the Senate Standing Committee.

[3] John Adams, "The Government of Canada and Cyber Security: Security Begins at Home," *Journal of Military and Strategic Studies* 14, no. 2 (2012): 26. While this chart refers specifically to cybersecurity, it is a good representation of the diversity of departments and agencies that can be involved in a given national security issue.

[4] Michel Coulombe, *Canadian Security Intelligence Service*. https://www.csis-scrs.gc.ca/index-en.php (accessed

June 29th, 2014).

5. Coulombe, *Canadian Security Intelligence Service,* https://www.csis-scrs.gc.ca/index-en.php (accessed June 29th, 2014).
6. Government of Canada, *Canada First Defence Strategy*, http://www.forces.gc.ca/en/about/canada-first-defence-strategy.page? (accessed June 29th, 2014).
7. Megan Warshawsky, “The balance to be found between civil liberties and national security,” *The RUSI Journal* 158, no. 2 (2013): 95.
8. Ferry de Kerchove and George Petrolekas, *The Strategic Outlook for Canada 2014*, Ottawa: Conference of Defence Associations Institute, 2014: 1.
9. de Kerchove and Petrolekas, *Strategic Outlook 2014,* 1.
10. Richard A. Clarke, and Robert K. Knake, *Cyber War*, New York: Ecco, 2012: 291 – 296.

11, David Sanger, “Obama Order Sped Up Wave of Cyberattacks Against Iran,” *The New York Times* June 1, 2012, http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&hp [accessed June 30th, 2014].

12. Clarke and Knake, *Cyber War.* 11 – 21.
13. *Ibid*., 50.
14. Joe Castaldo, “Spies like us,” *Canadian Business,* November 11, 2013: 39.
15. Angela Gendron, "Cyber threats and multiplier effects: Canada at risk, "*Canadian Foreign Policy Journal* 19, no. 2 (2013): 178.
16. *Ibid*.
17. *Ibid*.
18. Adams, "The Government of Canada and Cyber Security,” 1.
19. *Ibid*., 3-4.
20. *Ibid*., 2.
21. Jacques J. M.. Shore, "Intelligence Review and Oversight in Post-9/11 Canada," *International Journal of Intelligence and Counterintelligence* 19, no. 3 (2006): 462.
22. Security Intelligence Review Committee, “Frequently Asked Questions,” http://www.sirc-csars.gc.ca/faqfqs/index-eng.html (accessed June 30th, 2014).
23. *Ibid*.
24. Canadian Press, “Axing CSIS watchdog 'huge loss', says former Inspector General,” http://www.cbc.ca/news/politics/axing-csis-watchdog-huge-loss-says-former-inspector-general-1.1143212 (accessed June 30th, 2014).
25. Office of the Communications Security Establishment Commissioner, “Review Function,” http://www.ocsec-bccst.gc.ca/functions/review_e.php (accessed June 30th, 2014).
26. Shore, "Intelligence Review and Oversight in Post-9/11 Canada," 462.
27. *Ibid*., 462-3.
28. *Ibid*., 468.
29. Steven Penney, "National Security Surveillance in an Age of Terror: Statutory Powers & Charter Limits, "*Osgoode Hall Law Journal* 48 (2010): 274.
30. Jane Bailey, “Systematic Government Access to Private Sector Data in Canada," *International Data Privacy Law* 2 (2012): 219.
31. Penney, “National Security Surveillance,” 252.
32. Lorne Bozinoff, “Three Quarters Disapprove of Bill C-13.” *The Forum Poll* (June 19, 2014) http://poll.forumresearch.com/post/68/three-quarters-disapprove-bill-c13/ (accessed June 30th, 2014).
33. See the record of Meeting 18 of the House of Commons Standing Committee on National Defence, for exmaple: http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=6511518&Language=E&Mode=1&Parl=41&Ses=2.
34. Information and Privacy Commissioner of Ontario, “A Primer on Metadata: Separating Fact from Fiction,” http://www.privacybydesign.ca/content/uploads/2013/07/Metadata.pdf (accessed June 30th, 2014).
35. *Ibid*.
36. Forcese, "Law, Logarithms and Liberties," 5.
37. Jeff Tasseron, "Who Should Watch the Watchers? Disruptive Innovation and the Digital Divide," *On Track* 19, no. 1 (2014): 28.
38. Forcese, "Law, Logarithms and Liberties," 32.
39. Penney, "National Security Surveillance in an Age of Terror: Statutory Powers & Charter Limits," 285.

[40] Interviews with Rick Norlock and Jack Harris.

[41] Shore, "Intelligence Review and Oversight in Post-9/11 Canada," 468.

[42] Security Intelligence Review Committee, *Review and Oversight in the New Millennium: Challenges of a Multipolar World*, Proceedings of the Intelligence Review Agencies Conference, June 27-29, 1999, Ottawa. 16, 19, 25.

[43] Tasseron, "Who Should Watch the Watchers?" 28.

[44] *Ibid*., 29.