PART III

REFORMS AND ACCOUNTABILITY

Page left blank intentionally

CHAPTER VI

Permanent Accountability Gaps and Partial Remedies

Kent Roach

Introduction

Accountability gaps occur when those who review or oversee national security activities do not have the necessary legal powers or resources to keep pace with the enhanced and integrated nature of those activities. Both the Arar Commission in 2006 and the Air India Commission in 2010 sounded alarm bells that neither review or oversight was keeping up with whole-of-government-approaches to security. The Arar Commission,[1] in what was, until the early 2015 debates about Bill C-51,[2] a neglected six-hundred-page second report, recommended that review be extended to other security agencies and that the reviewers be able, like the security agencies themselves, to share information with each other and to conduct joint investigations. The Air India Commission recommended an enhanced role for the prime minister's national security advisor to oversee and resolve inevitable disputes between security agencies, especially the Canadian Security Intelligence Service (CSIS) and the RCMP.[3] The government rejected both these recommendations.

Now the accountability gap problem has come home to roost in the wake of the fallout from the October 2014 terrorist attacks in Saint-Jean-sur-Richelieu and Ottawa. The government has introduced Bill C-51, which will authorize whole-of-government information sharing for extremely broadly defined security reasons, but without

enhanced whole-of-government review.[4] The new legislation will also give CSIS new surveillance and disruption powers, including the ability to break Canadian and foreign laws and to conduct surveillance and disruption outside of Canada.[5] In recognition of the *Charter* implications of such new powers and perhaps also in recognition of the outdated and shaky nature of Canada's review structures, the government has assigned the task of reviewing and overseeing many of these powers to Federal Court judges. The government has stressed the importance of judicial oversight in defending the new legislation, raising squarely the question of the strengths and weaknesses of judicial review and oversight of national security activities.

The first part of the chapter will define what is meant by review, oversight, accountability, and accountability gaps to clarify thinking about these matters. The second part will examine the dangers of the permanent accountability gaps that are emerging between enhanced and integrated national security activities and their review and oversight. A lack of accountability can shelter misconduct, including human rights and privacy violations. It can also hide governmental inefficiencies and failures in protecting national security. The Arar and the Air India Commissions both recommended means of improving accountability. The Arar Commission focused on the propriety of national security activities, while the Air India Commission focused on the efficacy of national security activities. Both commissions were agreed, however, that review and oversight of national security activities were manifestly inadequate. The Harper government, unfortunately, has rejected the major recommendations of both commissions. It has even characterized enhanced review as "needless red tape"[6] in response to concerns that new information sharing powers in Bill C-51 are not matched by increased and whole-of-government accountability. It has also characterized legislative review as foreign to Canadian traditions and has stressed the superiority of judicial oversight, especially with regards to new CSIS powers.[7]

The third part of the chapter will examine proposals for enhanced legislative review of national security activities. Opposition parties, especially the Liberals, have made the need for enhanced parliamentary review the focus of much of their opposition to Bill C-51. Canada, alone of its Five Eyes security partners, does not allow even a select group of parliamentarians have access to secret information. There cannot be meaningful detailed review of security matters without access to secret information. But, as is often the case,

be careful what you wish for. Although enhanced parliamentary review might increase public knowledge and perhaps ministerial accountability, the record in other democracies and current proposals before Parliament do not provide grounds for optimism that legislative committees will be effective in promoting robust accountability.

What about judicial oversight? Judicial oversight is the main form of oversight offered in the expansion of CSIS powers in both Bills C-44[8] and C-51. Judicial oversight can have teeth in the right circumstances. Justice Mosley issued a scathing judgment when he learned that CSIS and Communications Security Establishment (CSE) had enlisted the help of Five Eyes foreign partners without statutory or judicial authorization. The government is appealing this decision to the Supreme Court.[9] Although the judiciary has been a more effective mechanism for propriety-based review than in the pre-9/11 past,[10] caution is in order when relying on judicial oversight. Justice Mosley was able to leverage his considerable expertise and his interest in reading reports of review agencies to discover that CSIS had gone beyond the terms of the warrant he issued, but this raises the question of whether judges will always be able to engage in similar monitoring. Federal Court judges will review the new CSIS powers in a warrant setting, where it is only the judge and the government lawyer in the room. Once a warrant is granted, there are unlikely to be appeals, and the national security context makes it unlikely the warrant will be reviewed when evidence is introduced in a criminal trial. Moreover, the new disruption warrants in Bill C-51 are based on the constitutionally radical premise that the judicial role is not to prevent *Charter* violations but to authorize them. Such authorizations, including judicial judgments about what limits on rights are proportionate and reasonable, are unlikely to be reviewed on appeal. Review bodies and parliamentary committees may be reluctant to question the ambit of judicial warrants, even if they have concerns that they have gone too far.

The fifth part of this chapter will suggest that the most important accountability mechanisms are located not in the legislature or the judiciary but in the executive itself. National security activities that are themselves dominated by the executive must be closely monitored from within the executive. This is consistent with the fundamental principle accepted by both the Arar Commission and President Obama's review committee[11] that review should mirror and match the activities being reviewed. In particular, effective review

of national security activities will require the initiative and secrecy associated with the executive, as opposed to the more public and responsive nature of both legislative and judicial review. Executive review can take many forms. CSIS used to have an Inspector General, an internal watchdog who reported on the legality of its operations. The CSE commissioner is an independent retired judge who reviews the legality of the work of CSE. Legality is an important aspect of propriety, but it can be under-inclusive. The government has taken much comfort in the CSE commissioner's repeated assurances, after each Snowden revelation about Canada, that CSE's actions remain legal because they have been not directed at Canadians. Conclusions of legality are only as good as the underlying law. Former CSE commissioners themselves have raised concerns about the CSE's enabling legislation enacted hastily after 9/11 and some of the broad interpretations that Department of Justice lawyers have placed on the law.[12]

The time may have come for fundamental reform to Canada's accountability architecture. In my view, what is now necessary is the creation of a new independent committee or "super SIRC" (Security Intelligence Review Committee) with jurisdiction to review all national security activities within the federal government. This committee, like the Arar Commission itself, should have the ability to see all secret information and to challenge governmental redaction decisions in court. A larger committee might require a full-time chair, more staff who can specialize in working with different agencies, and a composition that includes a broader cross-section of the public. Although formerly classified in the executive, review bodies can be seen as hybrid institutions that combine elements of all three branches of government, especially if retired judges are used as reviewers.

The last part of this chapter will suggest that even if a "super SIRC" and a parliamentary committee with access to secret information were created, it would not be enough. There would still be a need for "whole of society" accountability. In other words, there is a need for multiple layers of accountability, including ad hoc inquiries, investigative media, civil society, consumer activism, privacy-sensitive telecommunications companies, and whistle-blowers. The President's Review Group was correct to conceive of accountability in risk management terms and to draw on all branches of government,[13] but its proposals to stop leaks could decrease accountability in the future. Those proposals, along with other proposed new

legislation in the United States also rely on corporate and consumer resistance to surveillance in its proposals to allow the private sector, as opposed to government, to store metadata about communications. Social accountability will require greater consumer knowledge and activism in demanding that both governments and telecommunication companies respect privacy. My focus on social accountability reflects the need for democratic demands for reducing accountability gaps.[14] It also reflects the growing recognition of the importance of "civil society constitutionalism."[15]

The Need for Conceptual Clarity about Some Critical Distinctions and Definitions

Given the ongoing expansion of security powers and surveillance capabilities, it is understandable and healthy that many people are increasingly concerned about the adequacy of review and oversight of national security activities. Alas, much public discussion conflates the distinct meanings of review and oversight. Loose language and muddled thinking is a real danger. Without conceptual clarity at the start about the different ambitions of review and oversight, there will only be confusion and disappointment even if reforms are implemented.

Review and Oversight

Review refers to the ability of independent bodies retrospectively to evaluate security activities.[16] A reviewer does not have operational responsibility for what is being reviewed. This helps ensure that reviewers remain independent and are not complicit or seen to be complicit in what is being reviewed. SIRC, the CSE commissioner, and the Civilian Review and Complaints Commission for the RCMP are all examples of review bodies that conduct reviews after the fact. In addition to hearing complaints, they make findings and recommendations that attempt to foster accountability to the government and promote public trust and confidence.[17] They do not have the power to impose remedies on the agencies they review.

Oversight refers to a command and control process where those who practice oversight may be able to influence the conduct that they are examining.[18] The responsible minister is supposed to have an important oversight role in a parliamentary democracy. The minister of public safety is responsible for both the RCMP and CSIS. One

manifestation of ministerial oversight is the issuance of guidelines and directives to the agencies. Ministerial oversight of the police is limited by the constitutional principle of police independence over law enforcement decisions such as investigations, arrests, and charges.[19] The Arar Commission did not recommend oversight of the RCMP in part because such a role could interfere with police independence. It also expressed concerns that an oversight role that intruded on the management of the agency could compromise the independence of the review body by implicating it in the decisions being reviewed.[20]

Propriety and Efficacy

Distinctions are often drawn between review of the propriety and the efficacy of national security activities. The Arar Commission noted that independent review is generally concerned with propriety, including but not limited to, compliance with law. Some propriety-based reviews, such as the review of the proportionality of a measure, may touch on matters of efficacy and competence, but they are not the focus of such reviews. The Arar Commission suggested that questions about "the efficacy of the intelligence community as a whole… may be an appropriate subject for the proposed Parliamentary Committee on National Security."[21] Those who practice oversight, such as ministers, would also be concerned about efficacy, in part because they may have to answer for security failures.

Accountability and Accountability Gaps

Accountability refers to processes in which officials and organizations provide explanations and justifications for their conduct. A body can demand an accounting even if it does not have the power to control or change the behaviour for which it is demanding an explanation.[22] In other words, a review body that is not in the chain of command can still demand accountability. So too can those in the chain of command, such as ministers who have oversight powers. Accountability, like review and oversight, can relate to the propriety and/or the efficacy of conduct.

Accountability gaps occur when reviewers or overseers do not have adequate powers or resources to match the conduct that is being reviewed. All democracies post-9/11 are struggling with accountability gaps in national security matters. These gaps have been created as governments move to more intense and more integrated

"whole-of-government" national security activities, but without always ensuring that reviewers and overseers have corresponding enhanced whole-of-government powers and adequate resources to keep pace with what is being reviewed.[23] In other words, accountability gaps occur when reviewers and overseers remain stuck in twentieth-century silos, while security agencies escape silos in order to work with domestic and foreign partners.

Accountability gaps may have been created unwittingly at first, given the rapid response to 9/11, but their persistence many years later raises questions of whether it may be in the interest of governments to have them. Accountability gaps should be a matter of concern, because they create risks to both rights and security. The risks to rights are that whole-of-government activities may violate rights such as privacy, while the risks to security involve inefficient practices and security failures.

The Role of All Three Branches of Government and Hybrid Institutions

Matters are made even more complicated because all three branches of government can be engaged in review and oversight. Judges can review national security activities by means of judicial review and after the fact in the course of criminal or civil trials. They may be involved in oversight, for example, in ensuring that intelligence agencies properly execute warrants. Legislative committees generally are concerned with after the fact review, but in some extraordinary cases they can play a more hands-on oversight role. Finally, the executive in its many guises plays a variety of roles. Ministers are supposed to engage in oversight for both the efficacy and propriety of national security activities. In addition, watchdog executive bodies in the executive, such as SIRC and the CSE commissioner, engage in retrospective reviews of the propriety and legality of the conduct of CSIS and the CSE.

Although part of the executive, SIRC and the CSE commissioner are hybrid institutions. SIRC members are appointed by the prime minister, but in consultation with the leaders of major parties in the House of Commons.[24] Although SIRC members cannot be current members of Parliament, by convention, they often have had experience in the legislature and its political parties. More recently, they include retired judges and former civil servants. The CSE commissioner must be a supernumerary or retired judge.[25] This also brings a judicial element into the review process.

The Danger of Accountability Gaps for Propriety and Efficacy: The Rejected Arar and Air India Commission Recommendations

Accountability is often associated with the need to reveal and prevent improprieties such as possible complicity in torture and the massive privacy invasions revealed by the Snowden leaks. For example, the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar's extraordinary rendition and torture crafted its recommendations with a focus on reviewing for propriety while also noting that, in some circumstances, "issues of efficacy and propriety are interwoven, and comments about competence or capacity related to propriety will be highly useful and desirable."[26]

In contrast, the Air India Commission evaluated "how effectively the government uses the resources available to it to deal with the terrorist threat"[27] with particular attention to the distribution of intelligence and its relation to evidence. It recommended that CSIS (and by implication CSE) should no longer have an unreviewable discretion not to share relevant intelligence with others in government. Instead, it recommended that intelligence should be shared and protected by a new legislated privilege from disclosure until a decision was made by the prime minister's national security advisor about whether the intelligence should be more broadly shared within government, even at the risk of possible leaks or legal demands for disclosure. In essence, the PM's national security advisor would decide in the public interest among the competing demands that intelligence be kept secret or that it be used for prosecutorial or other purposes that would risk its disclosure. The government has shown little interest in this recommendation that would have increased and focused oversight and accountability at the centre for the efficacy of national security decisions.[28]

Accountability and Secrecy

Accountability is impossible to achieve if relevant information is kept secret from those demanding accountability. For this reason, the Arar Commission stressed that those who review national security activities should have access to all relevant information regardless of its classification. In addition, the secrecy of national security activities meant that reviewers should be able to conduct self-initiated reviews and not simply respond to complaints. It concluded that while SIRC and the CSE commissioner had such powers,

the commission reviewing the RCMP's national security activities lacked such powers. Subsequent legislation stopped short of the Arar Commission's recommendations because the RCMP's Civilian Review and Complaints Commission must go through an elaborate process involving an advisory opinion from a retired judge if the RCMP commissioner refuses to provide it with access to secret information.[29]

The Arar Commission also recommended that statutory gateways be created between the three review bodies for CSIS, CSE, and the RCMP so that the review bodies, like the security agencies themselves, could share secret information and if necessary conduct joint investigations. The government has refused to implement this recommendation, even while proposing in Bill C-51 to facilitate information sharing within government.

To be sure, the Arar Commission recognized that the government and reviewers may disagree over what information could be made public, but it stressed that these disputes should be resolved after review was conducted. Much of the work done by SIRC and the CSE commissioner remains secret and is submitted only to the minister. Given recent experiences of the government overclaiming secrecy, thought should be given to allowing review agencies to use section 38 of the *Canada Evidence Act*, as the Arar Commission did with some success,[30] to challenge the government's secrecy claims.

Given the time-sensitive nature of secrecy and the importance of publicity to accountability, some of the older but still secret review reports submitted by SIRC and the CSE commissioner to the minister of public safety should be considered for public disclosure. The United States has declassified much material in response to Snowden revelations, but Canada has not. SIRC lists close to two hundred secret reports submitted to the minister starting in 1986,[31] and the CSE commissioner lists over eighty classified reports since 1997.[32] Given the government's sustained practice of overclaiming secrecy, it is difficult to think that not one of these reports could be declassified.

The Values of Accountability

The lack of transparency and effective accountability for national security activities, including signals intelligence, creates dangers for both human rights and security. The immediate concern is often, as it has been in the wake of the Snowden revelations, on human rights abuses and invasions of privacy. At the same time, a lack of accountability can shelter inefficiencies or national security activities

that are counterproductive or not properly authorized. Much of the criticism of CSE spying on Brazil revealed by the Snowden leaks has been about the efficacy of such measures. Similarly, the Air India Commission largely accepted allegations by former security official James Bartleman that the predecessor of CSE had access to signals intelligence about the threat to Air India planes before the 1985 bombings that killed 331 people in the world's most deadly act of aviation terrorism before 9/11. Efficacy concerns cannot be ignored, given that it may be difficult and sometimes impossible to find actionable intelligence in the Big Data collected by the NSA and CSE.

Although accountability proposals do not command nearly as much attention as the underlying impropriety or inefficiency that leads to them, we should all be concerned about permanent accountability gaps in which intelligence agencies remain one or more steps ahead of their political masters, their reviewers, civil society, and the citizenry. To be sure, past accountability failures and an increasing cynicism about government makes many skeptical about accountability reform. The former CSE commissioner has dismissed the Arar Commission's proposals for enhanced accountability as "an additional super-bureaucracy, with the associated burden and costs."[33] Such statements have likely encouraged the Canadian government aggressively to characterize additional review as "needless red tape,"[34] even as it dramatically increases security powers in Bill C-51.

The Consequences of Shortchanging Review

Equating review with red tape is short-sighted. It ignores the dramatic increase in resources, intensity, and integration of national security activities since 9/11. One result is that the resources devoted to the review of national security activities have been dwarfed by the expanded budgets of intelligence agencies. For example, the CSE commissioner has an annual budget of around $2 million and ten full-time equivalents to review CSE, which has a reported budget of $350 to $422 million and almost two thousand full-time equivalents.[35] SIRC, with an annual budget under $3 million and seventeen full-time equivalents (down from twenty in 2006, despite the abolition of the Inspector General), reviews CSIS, which has over 3,200 employees and a budget of over $500 million.[36] The government has in its April 2015 budget committed to almost doubling SIRC's budget, but not to alter its lack of power to share secret information and conduct joint reviews.

Accountability gaps have implications for public confidence in and social license for security activities. Bill C-51's broad definition of the ambit of information sharing has set off alarm bells within Canada's Muslim community and among a broad range of Aboriginal, environmental, and separatist groups that may be subject to security information sharing. The Canadian government could more credibly rebut these concerns as alarmist if it had an adequately resourced, whole-of-government review body that could review information sharing. The government has argued that the Privacy Commissioner provides such whole-of-government review. But the Privacy Commissioner, in a 2014 report, raised concerns that it is operating under out-of-date legislation that does not give it adequate powers to share information and conduct joint reviews or have access to the Federal Court with respect to collection and disclosure of personal information that is classified secret.[37] Nothing in Bill C-51 responds to these recent concerns articulated by the Privacy Commissioner.

The accountability gaps that have emerged between whole-of-government security responses and their review and oversight are very troubling, especially in an era when the government is embarking on a second round of post-9/11 increases in security powers to respond to the real foreign terrorist fighter threat. Such gaps can harm rights, including privacy. There are also concerns about chilling expression and protests and discriminatory profiling and guilt by association reasoning. This, in turn, affects public confidence and social licence for intelligence and other security activities. Finally, accountability gaps can hurt security if they prevent independent reviewers from being able to see the big picture to determine whether the appropriate amount of intelligence is being collected and shared with whom ever it needs to be shared with in a timely and useful manner. These oversight concerns are particularly pressing given the increases in CSIS's powers and privileges under Bills C-44 and C-51 and the possibility that the new privilege for CSIS human powers and its new powers of disruption may have the unintended effect of making terrorism prosecutions even more difficult.[38]

Legislative Accountability: Be Careful What You Wish For

Canada, unlike its Five Eyes security partners, does not give any parliamentarians regular access to secret information. The Afghan detainee affair, in which Parliament had to hold the government

prima facie in contempt of Parliament to get any access to secret documents relating to whether former detainees were tortured after being transferred from the custody of Canadian Forces to Afghan officials, revealed this lack of access as a critical weakness. It resulted in struggles between the government and Parliament that saw Parliament prorogued in 2009 in the face of a motion demanding access. In addition, an ad hoc committee of retired judges and parliamentarians from all parties (except the NDP) was created to review secret documents in the wake of the Speaker's ruling on contempt. Despite this crisis, there has been very little interest in Canada in giving parliamentarians regular access to secret information. This may change after the opposition parties, especially the Liberals, make lack of parliamentary review the focus of their opposition to Bill C-51.

Current Reform Proposals

Most current proposals to give Parliamentarians access to secret information are quite modest and suggest that increased Parliamentary review will not cure Bill C-51's many ills. A private member's bill introduced by Liberal MP Wayne Easter was particularly anaemic. Not only would members of the proposed committee be permanently bound to secrecy by statute,[39] but the responsible minister would have final and non-reviewable power to decide how much, if any, secret information to provide the committee.[40] Such a deferential approach may be related to the novelty of giving Canadian parliamentarians any access to secret information. It may also reflect anxieties that Canada's oft-noted status as a net importer of intelligence renders it vulnerable to having the intelligence tap cut off by allies if secrets are leaked.[41] An often unspoken but real factor behind Canada's persistent fear of leaks is the concern that separatist or radical parliamentarians are less trustworthy. In any event, the Easter bill would do little more than give parliamentarians the most tentative toehold inside the secrecy tent.

Another private members' bill, sponsored by Liberal MP Joyce Murray, had more robust powers to access secret information, but it was defeated by the government in October 2014. This bill also took a multi-pronged approach to accountability and attempted to increase judicial and ministerial oversight of CSE as well as the oversight role of the CSE commissioner.[42] It will be suggested in the conclusion that such a multi-pronged approach is indeed necessary if we are to close accountability gaps.

Some commentators have criticized the Arar Commission for not including enhanced parliamentary reform within their proposals.[43] In my view, such criticisms are unfair, given the commission's mandate, which focused on review of the RCMP's national security activities. In any event, such criticisms overestimate what can be achieved through parliamentary review. The experience of other democracies with legislative review suggests the contributions of parliamentary review are likely to be modest. This is especially so given that Canadian committees are poorly staffed, the high turnover rate among parliamentarians and the haphazard nature of their knowledge and interest in security matters.

The Intelligence and Security Committee (ISC) in the UK is often held up as an example, but Canadian accounts of the ISC often discount UK criticisms of its performance on sensitive issues, including possible complicity in torture. The performance of legislative review in the United States has been, if anything, even less inspiring than in the UK. Various members of Congress were briefed on the activities of the NSA after 9/11 but it took the *New York Times* in 2005 to reveal President Bush's illegal orders for NSA domestic spying and then the Snowden leaks to reveal the NSA's more recent activities.

American legislative committees are much better staffed than Canadian ones, but there are still concerns that legislators in Congress often lack the expertise or the budgetary powers to conduct effective oversight.[44] Giving legislators access to secret information but no mechanism to disclose it may only allow the government to claim legitimacy for illegal and improper conduct because some legislators had been "briefed in" to the activities. Some American commentators have made interesting recommendations that would give opposition parties with access to secret information powers to push for the declassification of documents,[45] but there has been little uptake on such proposals. A committee with access to secret information could question ministers and officials *in camera*, but it could not make secret information public even if the information had been over-classified as secret.

What Do We Want from Enhanced Parliamentary Review?

More thought needs to be given to exactly what we want from enhanced legislative review. The Afghan detainee issue shows that parliamentarians may be concerned about propriety, albeit with a distinctly partisan edge. The opposition maintained interest in

whether Canadian Forces had been complicit with torture for an extended period of time, but interest in this issue eventually died down. Most other security matters will be considerably less dramatic. Parliamentary accountability may ultimately depend on the degree of interest and knowledge about security matters in the media and civil society, matters to be discussed in the last part of this chapter.

A parliamentary committee with access to the many confidential reports that review bodies provide to ministers could hold the ministers to account for their response to those reports. It must be understood that review bodies such as SIRC and the CSE commissioner only have powers to make non-binding recommendations to the minister and the agencies. A parliamentary committee would be able to demand explanations from the responsible ministers but would not have oversight or chain-of-command powers to force the minister or the agency to take remedial action.

A parliamentary committee could address efficacy issues that may be downplayed by other review bodies. For example, it could help ensure that ministers can be held accountable for controversial forms of surveillance such as CSE's spying in Brazil.[46]

A national security committee at present would have to require both the minister of public safety and the minister of defence responsible for CSE to explain their actions. There may be a case for making the minister of public safety responsible for all non-military aspects of intelligence so that ministerial accountability for intelligence is not diffuse.

Any proposals for increased parliamentary review must confront the fact that Canadian committees do not have the same research capacities as American or British committees. The Privacy Commissioner's recent proposal that parliamentarians conduct "a global study of Canada's intelligence oversight and review mechanisms"[47] ignores the limited resources of parliamentary committees even when assisted by the Library of Parliament. It also ignores that much of this work has already been done by the multimillion-dollar Arar Commission in its neglected second report.

Some claim that a parliamentary committee might make security issues less partisan, but there are no guarantees. Bill C-51 was introduced by Prime Minister Harper in an election style rally in January, 2015, and not in Parliament. The way the Afghan detainee affair was handled was also quite partisan on all sides. It is also not certain that parliamentary committees will increase public

confidence in our security responses, especially because confidence in both elected members of Parliament and the unelected Senate seems at an all-time low. Rather than relying on its members, much of the legitimacy of a parliamentary committee might come from its engagement with civil society and the media. Any parliamentary committee will have to win public confidence through its work.

Increased parliamentary review might help increase parliamentary and public knowledge of security matters. At the same time, the challenges for parliamentarians, especially those in the Commons, of mastering security matters should not be underestimated. For example, Bill C-51 lists seventeen different departments and agencies that could receive security information. It will create two new security statutes on information sharing and the no-fly list, and it will amend fifteen other acts, including the *CSIS Act*, the *Criminal Code*, and the *Immigration and Refugee Protection Act*. Will parliamentarians be able to stay on top of this mass of laws, let alone understand how they are enforced? To be sure, we need enhanced parliamentary review with access to secret information, but it would be a serious mistake to expect too much of that process.

Judicial Accountability: Into the Breach or Creating the Breach?

The Arar Commission was not optimistic about relying on judicial review of national security activities because "the judiciary is a reactive institution" that can only respond to misconduct when it becomes the subject of litigation. It warned that, because of secrecy, "affected individuals may never know that they have been subject to a national security investigation. This reduced level of judicial oversight is a further reason for independent review."[48] Even if individuals do have such knowledge, they may not have the resources to bring a court challenge. And even if they do have the resources, they will face great secrecy barriers in their litigation. Finally, the comparative lack of prosecutions in the national security area means that the courts provide "less oversight" for national security investigations "than they do for other criminal investigations."[49]

There are, however, some virtues of involving the judiciary in review and oversight. The judiciary's traditional deference on national security matters has eroded in the wake of post-9/11 security abuses. Gone are the days when judges would not even look at secret information, and courts in Canada and elsewhere have pushed back

on a number of fronts in the post-9/11 era. The judiciary has been at its strongest in insisting on greater transparency where secret information has been used. Particularly noteworthy are Supreme Court decisions insisting on retention of raw intelligence investigating specific individuals, adversarial challenge to such intelligence, and insistence on minimal disclosure in security certificate cases.[50] Another precedent that may be particularly relevant in the era of foreign terrorist fighters is a Federal Court decision upholding the right of a Canadian citizen to return to Canada even though he was at the time listed by the UN as affiliated with al-Qaeda.[51]

Justice Mosley's Decision on the Outsourcing of Surveillance to Five Eyes Partners

Judges can be tenacious in ensuring that security agencies do not go beyond the scope of what they have authorized. In 2009, Justice Mosley issued warrants to allow CSIS to intercept foreign communications of Canadian citizens. In August 2013, upon reading the annual public report of the CSE commissioner, he convened a new hearing on his own initiative. He was not happy.

Justice Mosley concluded that CSIS had misled him by not revealing its plans to draw on the assistance of CSE's Five Eyes signals intelligence partners in carrying out the surveillance. He called this a "deliberate decision to keep the Court in the dark about the scope and extent of the foreign collection efforts that would flow from the Court's issuance of a warrant."[52] He also concluded that the tasking of foreign agencies by Canadian officials to conduct the surveillance was unlawful. He was concerned that the warrants he'd granted had been used as "protective cover."[53]

What happened in this case was not an isolated occurrence. Drawing on a SIRC report, Justice Mosley noted that foreign assets had been used in as many as thirty-five warrants issued since 2009. Justice Mosley warned that Canada could lose control of intelligence it asked its foreign partners to collect. He underlined the grave risks when Canada loses control over its own intelligence with reference to the role that Canadian information and requests for foreign assistance had played in the torture of Maher Arar and other Canadians in Syria.[54]

Justice Mosley's extraordinary decision provides a rare glimpse into the Five Eyes relationship, normally one of Ottawa's most closely guarded secrets. Justice Mosley ruled that no reference should be

made by CSIS, CSE, or its legal advisors to the erroneous idea that a CSIS warrant authorized the tasking of foreign agencies. He read down Canadian laws so as to prevent a transnational accountability gap that would occur if Canada tasked foreign agencies to conduct surveillance of Canadian targets in a manner that effectively left Canada without control of the intelligence produced by its own targeting and tasking. Judicial attempts to plug and stop accountability gaps are welcome, but they will generally only occur when states attempts to abuse judicial authority and engage in blatant misconduct. Indeed, much of Justice Mosley's bold judgment was premised on the assumption that Canadian tasking of surveillance by its Five Eyes partners would violate international law.

Justice Mosley also recognized the need for continual review by executive watchdog agencies, review that he had benefited from. To this end, he required that a copy of his decision be provided to both SIRC and the CSE commissioner. This judgment, like some of the American Foreign Intelligence Surveillance Court (FISC) decisions declassified in the wake of the Snowden leaks, demonstrates how judges can complement the review process but also how they may depend on executive watchdog review.

The federal government might point to the Justice Mosley decision as exhibit A revealing the strength of the judicial oversight that will be required when Federal Court judges consider CSIS warrant requests for otherwise illegal conduct under Bills C-44 and C-51. One problem with such an approach is that the government is appealing Justice Mosley's decision all the way to the Supreme Court. If the government wins in the Supreme Court, CSIS may not have to bother with warrants with respect to investigations outside of Canada.

The Supreme Court's decision to hear the government's appeal opens up the possibility that the court might say that warrants are not required for some extraterritorial CSIS investigations. Such a ruling would allow CSIS to act without warrants and without the judicial oversight that the government has promised in its defence of Bills C-44 and C-51. Conversely, the court might uphold Justice Mosley's judgments in even more ringing and emphatic terms than the Federal Court of Appeal. That would be good, but we should not underestimate how much the judgment depended on heroic levels of knowledge and initiative of one judge with a particularly long history of expertise in national security matters.

Judges Being Asked to Approve and Oversee Breaches of the Law and the Charter

Federal Court judges will soon be able, under both Bills C-44 and C-51, to grant warrants "without regard to any other law, including that of a foreign state."[55] Under Bill C-51 as introduced in Parliament, judges will even be able to grant CSIS a warrant to contravene the *Charter* provided that the proposed measure is proportionate to the threat and the reasonable availability of other measures to reduce the threat[56] and provided it does not intentionally or negligently inflict death or bodily harm, invade sexual integrity, or obstruct justice.[57] Bill C-51 builds on the pattern in Bill C-44 of allowing Federal Court judges to authorize CSIS to break domestic and foreign laws, but it goes a step farther by providing that CSIS may also obtain a judicial warrant to reduce a threat to the security of Canada in a manner that will contravene *Charter* rights.

The government is defending Bill C-51 by stressing that the powers will be subject to judicial oversight. Minister of Defence Jason Kenny has even argued that Bill C-51 "doesn't give new powers to police or intelligence agencies but rather to judges, to courts."[58] This ignores that CSIS will execute the warrants and that Justice Mosley's decision provides some grounds to be concerned about whether CSIS will go beyond what is specifically authorized in the warrant. It downplays the radical implications of a single judge authorizing a violation of the *Charter* in a warrant context where the decision is not likely to be reviewed in subsequent trials or on appeal.

Bills C-44 and C-51 are silent on what, if any, accountability measures Federal Court judges will provide to ensure that security agencies do not go beyond the terms of new warrants. Justice Mosley's judgment suggests that judges may not tolerate activity beyond what they have authorized *if they find out about it*. It is not comforting, however, that it appears to have been Justice Mosley's extracurricular reading of the reports of review bodies that led to the discovery that CSIS had subcontracted surveillance to foreign allies.

The nature of CSIS warrants means that the appropriateness of the limits that they set will not be generally tested on appeal. Warrant proceedings are generally one-sided proceedings. Although a security cleared *amicus* was appointed on some of the legal issues before and after Justice Mosley's warrant, that is not the norm and it is not specifically provided for in either Bill C-44 or C-51. Moreover, as the Arar Commission stressed, national security activities are much less

subject to judicial review than ordinary warrants. Indeed, the leading appeal decision on CSIS warrants dates back to 1987.[59] In the wake of the Snowden revelations, the Privacy and Civil Liberties Board in the United States recommended that the Foreign Intelligence Surveillance Court (FISC), which also grants warrants *ex parte*, should be assisted by security-cleared special advocates. It also recommended that efforts should be made to encourage both more appeals from the warrants and more declassification of FISC decisions.[60]

Craig Forcese and I have raised concerns about wording in Bill C-51 that allows Federal Court judges to authorize *Charter* violations in the course of issuing CSIS warrants to reduce security threats.[61] In our view, this would be an unprecedented grant of power to judges to authorize *Charter* violations, as opposed to attempting to avoid *Charter* violations.[62] The grant of search warrants is traditionally seen as a method to avoid a violation of the right against unreasonable search and seizure under section 8 of the *Charter*. In contrast, a judge under Bill C-51 could authorize CSIS to take steps that will contravene a person's *Charter* rights, such as the right of citizens under section 6 of the *Charter* to leave or return to Canada.

The reasoning of Federal Court judges in warrant applications may for valid operational reasons relating to national security, national defence and foreign relations be kept secret for a long time. If released, such judgments may be heavily redacted. The leaked and declassified FISC decisions in the United States reveal that some of the credibility and trust that the judiciary enjoys may be undermined by secret jurisprudence, especially if it authorizes illegal and rights invasive conduct by intelligence agencies.

Professor Forcese and I also raise concerns that judges will be forced to make these difficult decisions in closed *ex parte* proceedings with at most security-cleared *amici curaie* (who are not specifically contemplated in the new warrant regime but are under proposed American reforms) playing a challenge role. Judges trained in an adversarial system may also not have the information and resources they need to ensure CSIS and those who assist them such as the CSE act in the manner specified in the warrant. Bill C-51 does not even ensure that the judge will know who CSIS asks to assist them in executing a threat reduction warrant. Nothing stops CSIS, especially when it acts outside of Canada, from enlisting foreign individuals and agencies.

The new warrant regime could change the role of the Federal Court, especially if the judges require the security agencies regularly

to report back to them about operations. The specially designated judges of the Federal Court may become something more akin to specialized investigating magistrates used in the French and other civilian systems. Such a "hands on" and potentially "dirty hands" role could compromise the impartiality and independence of judges who have authorized illegal activities that violate the *Charter*.[63] Even if the judges come down hard on CSIS misconduct, judicially supervised CSIS investigations may not have the disciplinary effects of criminal trials, in part because many judgments may remain secret for operational reasons.

The Federal Court is guided not by *Criminal Code* concepts based on guilt or innocence, but by the more expansive definition of threats to the security of Canada. It is noteworthy that the Supreme Court, when upholding investigative hearings, took care to insist that judges observe the normal rules of evidence and the presumption of open courts. Moreover, two judges dissented on the basis that it was alien to our system to have judges preside over police investigations.[64] It would be even more alien to have judges preside over CSIS illegalities and *Charter* violations committed at home and abroad.

Under Bills C-44 and C-51, Federal Court judges are being called into the breach with respect to devising accountability structures for CSIS. They are also being called to create breaches in the form of pre-authorized violations of Canadian and foreign laws and the *Charter*. They will be asked to create ad hoc accountability structures for CSIS to ensure that it respects the limits of judicial orders when violating laws and *Charter* rights both at home and abroad. To be sure, Bill C-51 places some categorical limits on what can be authorized: the measures must be reasonable and proportionate,[65] and they must never cause intentional or negligent bodily harm, violate sexual integrity, or wilfully obstruct justice.[66] At the same time, however, these limits will be observed in warrant decisions that may authorize violations of the *Charter* and other laws; that will be difficult to appeal and that may remain shrouded in secrecy.

The government seems happy to enlist judges under Bill C-51, but the result may strain the capacities of even the most able and dedicated judges. If things go wrong in the execution of one of these warrants at home or abroad, the result could tarnish the reputation of the judiciary while at the same time providing CSIS with protective cover. The government is defending Bill C-51 by stressing the role that judges will play, but the warrant process defies public

expectations that judges will act in a transparent and appealable manner after having heard adversarial argument from both sides. Finally, it asks judges who are supposed to uphold the law and the *Charter* to authorize and take responsibility for their violation by an intelligence agency.

Enhanced Executive Watchdog Review: The Need To See and Review the Big Picture for Propriety and Efficacy

Although legislative and judicial accountability mechanisms are needed, the most important mechanisms for holding intelligence agencies to account are those found within the executive. In Canada, these mechanisms include the role of retired judges as commissioners for the CSE, with broad public inquiry powers, and the ability of SIRC to have access to all secret information, except Cabinet confidences, held by CSIS. Both review mechanisms are hybrids between the executive and other branches of government. In the case of the CSE commissioner, the review body borrows from the brand of the judiciary with respect to independence and impartiality, and in the case of SIRC they borrow on the brand of the legislature in ensuring representation from all major political parties. Like other parts of the executive, they can be tasked by and report to responsible ministers and their number of classified reports directed to ministers is much greater than their number of annual public reports.

The Arar Commission stressed that any credible review mechanism for propriety should have unrestricted access to secret information and the ability to initiate its own audits or investigations. It was not opposed to review bodies hearing complaints, but recognized the limits of such mechanisms given the secrecy of most national security activities. After much deliberation, the commission opted for a model that would see a significant expansion of SIRC's mandate to include the national security activities of Citizenship and Immigration Canada, Transport Canada, the Financial and Transaction Report Analysis, and the Department of Foreign Affairs. A revitalized RCMP complaints agency would have jurisdiction to review the national security work of the Canada Border Services Agency. It also recommended that statutory gateways be created between three review agencies, SIRC for CSIS, the commissioner for CSE, and the RCMP review body. Finally, a coordinating committee composed of the chairs of the three main review bodies with an independent chair

would play a role in coordinating reviews and ensuring that there were not duplicative reviews of national security activities where the RCMP, CSIS, and CSE had overlapping responsibilities. All of these recommendations recognized the need for whole-of-government review to match whole-of-government security responses. At the same time, the commission ultimately opted for maintaining expertise by recommending that an expanded SIRC, the CSE commissioner, and a new RCMP review body all remain in place. It thus rejected proposals made to the commission for the creation of one big review committee or "super SIRC" that could review all national security activities.

The Changing Review Environment since the Arar Commission

The accountability gaps that the Arar Commission identified in 2006 have gotten worse since that time. The government reformed the RCMP review body but stopped short of giving that body full access to secret information by setting up a costly advisory process of retired judges mediating disputes about access to secret information. The government also rejected the recommendation that there be statutory gateways so the three review bodies could share secret information and conduct joint investigations. The government has not expanded review to cover the five other agencies with important national security responsibilities. Indeed, the government has even contradicted review by abolishing CSIS's Inspector General who served as the Minister's eyes and ears in CSIS and determined the legality of CSIS's actions.

In 2006, it was realistic to expect that the new Conservative government with its commitment to strengthening parliamentary review might adopt some version of Prime Minister Martin's 2005 proposals for a national security committee of parliamentarians. The Afghan detainee affair strengthened the case for a parliamentary committee with access to secret information, but the government was content to rely on a special ad hoc process. The government's largely successful obstruction of Parliament on that issue suggests that the prospect for parliamentary review has diminished. The government also refused to appoint a public inquiry as a means to make up for deficiencies in legislative and executive review as was done in the cases of Maher Arar and other Canadians tortured in Syria. The most recent indication that parliamentary review is not likely are attempts by the government in the Bill C-51 debate to paint

it as American and foreign to parliamentary systems.[67] This may simply reflect common and erroneous conflation of retrospective review with chain of command oversight, but it does not bode well for increased parliamentary review.

SIRC's brand has been diminished by the exploits of Arthur Porter, who resigned in late 2011 after his ties to the government of Sierra Leone were revealed. In early 2014, the public learned that three members of SIRC had financial ties to pipelines. Chair Chuck Strahl eventually resigned over the controversy.[68] I do not wish to impugn in any way the integrity of Mr. Strahl or other members of SIRC. They serve part time and are paid at rates well below what they would receive in the private sector. Nevertheless, the fact that a majority of SIRC members in 2014 had ties to pipeline companies makes it difficult for SIRC to command public confidence when it reviews CSIS's surveillance of those who oppose the pipelines, including environmentalists and Aboriginal groups. At the same time, it should be noted that the latest SIRC annual report was particularly hard-hitting and raised concerns about difficulties in obtaining information from CSIS and that several new appointments have been made to SIRC, including a retired judge, an academic, and a former civil servant, all professions associated with independence.[69]

The office of the CSE commissioner has escaped the scandals that have plagued SIRC, but its performance in response to the Snowden leaks has been questionable. On 13 June 2013, just a week after the first Snowden leaks, then Commissioner Décary issued a statement explaining his role of independent review and assuring the public that CSE was acting legally. He verified "that CSEC [CSE] does not direct its foreign signals intelligence collection…at any person in Canada," that it is "prohibited from requesting an international partner to undertake activities that CSEC itself is legally prohibited from conducting," and "that CSEC complies with any limitations imposed by law on the agency to which CSEC is providing assistance, for example, any conditions imposed by a judge in a warrant."[70] This statement would prove controversial in light of Justice Mosley's decision, released in December 2013. Commissioner Décary's 13 June 2013 statement also provided that he had "reviewed CSEC metadata activities and have found them to be in compliance with the law and to be subject to comprehensive and satisfactory measures to protect the privacy of Canadians."[71] This statement would be relied upon and prove controversial in light of subsequent Snowden leaks about metadata.

In an annual report dated June 2013 but released on 21 August 2013, Commissioner Décary verified that he had examined CSE assistance to CSIS in carrying out the warrant and that "CSEC conducted its activities in accordance with the law and ministerial direction, and in a manner that included measures to protect the privacy of Canadians."[72] The commissioner did, however, recommend that "CSEC advise CSIS to provide the Federal Court of Canada with certain additional information about the nature and extent of the assistance CSEC may provide CSIS."[73] This opaque and carefully worded reference did not retract the commissioner's assurance made earlier that month and in the annual report that CSE had complied with legal limits on its authority. Although the commissioner's recommendation, as well as the SIRC report, played a role in triggering Justice Mosley's re-evaluation of the warrants he had granted, the CSE commissioner's approach stopped short of ringing alarm bells. The commissioner's public performance is not nearly as robust as Justice Mosley's subsequent judgment, which concluded that CSE's activities were not authorized by his warrant or any legislation. In other words, they were illegal.[74]

The tension, if not the inconsistency, between Commissioner Décary's conclusion and those of Justice Mosley about the legality of CSE conduct are troubling, especially because the commissioner is limited to reviewing the legality of CSE activities. Former CSE commissioners, former Chief Justice of Canada Antonio Lamer and former Supreme Court Justice Charles Gonthier, expressed concerns about the way CSE and their Department of Justice advisors interpreted CSE's enabling legislation.[75] Conclusions of legality can mask disputed and complex questions of law. It does not assist public confidence that many of these disputes about legality may be sheltered from public exposure, given claims of both national security confidentiality and solicitor-client privilege.

Within a day of the story breaking that CSE had collected metadata from people using Wi-Fi in a Canadian Airport, CSE Commissioner Plouffe issued a press release stating, "In light of the most recent unauthorized disclosure of classified information of the Communications Security Establishment Canada (CSEC), I can state that I am aware of the metadata activities referred to." He noted that past commissioners had "reviewed CSEC metadata activities and have found them to be in compliance with the law and to be subject to comprehensive and satisfactory measures to protect the privacy of Canadians."[76]

Although Commissioner Plouffe's statement stopped short of declaring the airport program lawful, the government used these conclusions to defend CSE and to argue that the program "only" collected metadata and that the collection was not directed at Canadians in violation of CSE's legal mandate. Others argued that the program exceeded CSE's mandate and stressed the harmful effects on privacy of collecting metadata.[77] The commissioner's focus on legality downplayed the concerns about the effect of such activities on privacy.[78] A few weeks later, on 12 February 2014, the CSE commissioner issued another press release. It concluded that "CSEC activity does not involve 'mass surveillance' or tracking of Canadians or persons in Canada; no CSEC activity was directed at Canadians or persons in Canada."[79] The former conclusion responded to media concerns about the Snowden leaks, while the later tracked the language of CSE's enabling legislation.

CSE's enabling legislation was hastily enacted after 9/11 and it only prohibits surveillance that is "directed at Canadians or any person in Canada."[80] This legislation is being challenged under the *Charter*,[81] and indeed it seems to be at odds with fundamental *Charter* principles that suggest that the government can violate the *Charter* if its actions have the effect, even the unintended effect, of violating rights, including privacy. In other words, the fact that government actions are not designed for the purpose of violating the *Charter* does not necessarily mean that they are consistent with the *Charter*.

The commissioner's response to the Snowden revelations was defensive of the review status quo, asserting that its resources were adequate to review CSE and consistent with those of other agencies. The commissioner also affirmed that he would not allow embarrassing information to be taken out of his report. This, however, avoided the question of whether embarrassing information could be classified as secret and the lack of transparency of the process used to determine how much of the Commissioner's reports is classified.

The Need for a Super SIRC with a Whole-of-Government National Security Mandate

Increased security powers under Bill C-51, especially broad information sharing powers under the proposed *Security of Information Sharing Act*, as well as mandates to CSIS to act abroad in violation of Canadian and foreign law, suggest that the time has come for fundamental reform of Canada's review structure. SIRC was a

state-of-art institution that Canada could be proud of in 1984, but thirty-one years later it is showing its age. SIRC's powers of access to information are limited to the CSIS silo. The countervailing whole-of-government approach is epitomized in the proposed *Security of Canada Information Sharing Act*, which would allow any federal institution to share security information with seventeen different departments, many of which are subject to no independent review. The government has insisted that the existing review structures are up to the task.[82] Unfortunately, this ignores the stovepiped nature of existing reviews for CSIS, CSE, and the RCMP, and the limited mandate and powers of the Privacy Commissioner, underlined most recently in a 2014 report which found that its powers were not up to the task of reviewing information-sharing in the security context.[83]

All of these developments suggest that the time has come for more major reform than was recommended by the Arar Commission. There is also a need to respond to perceptions and at times realities of duplicative reviews that are often only a symptom of archaic twentieth-century stovepiped review functions.[84] In other words, the time has come to replace SIRC, the CSE commissioner, and that part of the RCMP review agency that reviews its national security activities, with one big committee or "super SIRC."[85] The new committee should ultimately have jurisdiction to review all of the government's national security activities, including security related information sharing.[86] Such an approach would have the virtue of allowing such a committee to follow the trail of intelligence, information sharing, and other national security activities throughout government without the need for statutory gateways.

A one-committee approach could also create possibilities for increased resources, full-time members, and broader representation of expertise and interests on the committee. One of the successful features of Canada's existing review mechanisms is that, while situated in the executive, they are hybrid institutions, with both the CSE commissioner and public inquiries benefiting from the presence of retired or sitting judges and SIRC having the advantage of representing former parliamentarians from all the major political parties. A new committee might include these elements,[87] but also include better representation from civil society in partial recognition that the existing parties do not command the same type of support from the public, and especially the young, as they once did. Thought should be given to creative ways to recruit and appoint members of such a

committee. There may also be a case for term limits, to prevent any perception or reality of capture. At the same time, staged appointments and staged expansion of a super SIRC's mandate could help ensure necessary expertise and experience. Those who serve either permanently or part-time on such a committee should be prepared to cut ties that may lead to reasonable perceptions of conflict of interest. Such a diverse committee should ideally have resources to hold public hearings and contribute to public education in a way that existing review bodies are unable to do.

A larger, more diverse and better-resourced super SIRC could also open up room for expertise of various forms and could expand review to include not only questions of legality but broader questions of propriety and even efficacy. Even with respect to propriety, it would be important that any new committee, unlike the CSE commissioner, not be restricted to reviewing the legality of actions. Retired judges are well-suited to making conclusions about legality, but such conclusions are only as good as the underlying law. The CSE commissioner's conclusions about legality have understandably been couched in terms that mirror the language of its enabling statute quickly enacted after 9/11. As discussed above, the commissioner has often stressed that CSE activities are not "directed" at Canadians or persons in Canada and that the information it collects is used for the "purpose of foreign intelligence." To be sure, these phrases mirror those found in section 273.64 of the *National Defence Act* defining the mandate of CSE, but it is far from clear whether they are sufficient to maintain public confidence in the face of the staggering Snowden revelations.

Indeed, a case may be made that CSE's mandate may already be out of date and insufficient to ensure privacy. For example, its focus on CSE's purposes in obtaining foreign intelligence are at odds with fundamental *Charter* principles that stress that government's conduct may be unconstitutional because of its effects on persons even if the purposes animating the state are entirely proper. The tension between the purpose-based statutory framework and the effects-based *Charter* framework has only been increased by the Supreme Court's recent decision recognizing privacy and anonymity interests in metadata.[88] Conclusions of legality are only as good as the underlying law.[89] Review for propriety should not be limited to legality. Conclusions of legality also echo the unfortunate torture memo experience where security agencies took comfort in secret and unreasonable legal opinions to provide protective cover for

problematic practices. Lawyers routinely disagree over matters of interpretation and some CSE commissioners have been unhappy with how Department of Justice lawyers have interpreted CSE's enabling statute.[90] Propriety issues including privacy are too important to be left to lawyerly sparring.

Although it focuses on propriety, the US Privacy and Civil Liberties Oversight Board has also been concerned about questions of efficacy and argues that the government should attempt to measure efficacy.[91] It has also held public hearings in a way that Canadian review bodies have not. It remains to be seen how the Privacy and Civil Liberties Board created under new British legislation will work,[92] but its creation is another sign that Canada is falling behind other democracies with respect to review of national security activities.

Any new watchdog and review body must have sufficient legal powers and resources to make progress on closing the accountability gaps that are increasing with increased legal powers and technological capacities for surveillance. A new review body requires a whole-of-government mandate and an ability to access the increasing amount of material that is classified as secret as government invests more in intelligence and secrecy. A new review body, like the Arar Commission, should not only have access to all relevant material regardless of its classification, but it should also be able to bring a court challenge to refusals by the government to allow it to publish part of its reports. Such challenges should be rare, but they would give the committee more power in dealing with the security agencies. Court challenges would provide a much more transparent process than that which governs the negotiations that apparently go on between SIRC and CSIS and the CSE commissioner and CSE over what material can be made public. Another alternative would be to allow a super SIRC to submit its classified reports to a parliamentary committee that could both the use the report in questioning ministers and officials and might be able to take steps to challenge the secrecy classification.

It is, of course, highly unlikely that a super SIRC will be adopted. The security establishment in Ottawa, as in other countries, has much leverage. In Canada, this leverage is increased by concerns that enhanced accountability may result in disclosures that could threaten intelligence-sharing relationships with foreign agencies. The time to fundamentally reform review structures was not in the

quasi crisis that have followed the October 2014 attacks and the Paris and Copenhagen attacks in early 2015, but in the quieter years after the Arar Commission's 2006 report. The government has prioritized giving security agencies and especially CSIS more power in Bills C-44 and C-51. Once they are enacted, there may be little incentive or energy to revisit the neglected question of review.

Whole of Society Review and Whistle-Blowing

Even if a super SIRC with adequate powers and resources were created, it would not be enough. As Michael Geist suggests in his chapter in this collection, we cannot just focus on watching public surveillance agencies but must be concerned about their corporate partners.[93] In addition civil society, the media and even whistle blowers all have a role to play in narrowing accountability gaps.

Corporate Accountability

The President's Review Group helpfully recommended that corporations publish more data about the information they provide to government. Legislative proposals related to the *USA Freedom Act* contemplate that corporations will hold domestic metadata and be able to challenge governmental requests for various forms of information. This raises the question of whether corporations will resist giving the government data. Ultimately this may depend on whether consumers and citizens will demand increased privacy protection from corporations. To what extent is there a market demand for privacy? There are many reasons for Blackberry's decline, but it is an interesting question whether its decision to co-operate with the government of India to allow a backdoor into its once-secure devices is one of them.[94] The power of corporations should not be underestimated. In the end, corporations will be driven by consumer demand and much will depend on how much consumers value their privacy.

Social Accountability

Both security and review of security are complex matters. Polls suggest that a large amount of the Canadian public are supportive of increased security powers but also want to see enhanced review and oversight.[95] The Canadian government seems to be promoting the idea that courts can be relied upon to ensure propriety-based

review of CSIS's increased powers. They also point to SIRC, the CSE commissioner, the RCMP review and complaints body, the Privacy Commissioner, and the Auditor General as evidence that there is enough review. The impression and sometimes the reality of duplicative and overlapping review may create review fatigue. There was no pressure on the government to respond to the Arar Commission's 2006 findings that the present review structure was inadequate. The Bill C-51 debate in early 2015 fortunately placed more emphasis on review. An impressive list of former prime ministers, judges and reviewers all wrote a public letter that echoed the Arar Commission's conclusions that the present review structure is inadequate.[96] Unfortunately, however, the government has only responded by increasing SIRC's budget, but not its jurisdiction.

If public demands for effective propriety-based review are not effective, perhaps demands for efficacy-based review may be. The Air India Commission stressed the need for better oversight of security and especially a need to resolve both historical and contemporary tensions between the RCMP and CSIS. CSIS has from its inception insisted that it does not collect evidence and the RCMP has facilitated this approach by relying as little as possible on CSIS information. This was a damning indictment of the system, but most of the fundamental reforms that the Commission recommended to improve the transition from intelligence to evidence have been rejected. Even in the wake of the October 2014 attacks, the public seems to be placated with the government's assurances that giving the police and especially CSIS more powers and privileges will be sufficient.

Accountability for both the propriety and efficacy of security activities will depend on public knowledge and demands. There is a need for civil society, the media, parliamentarians, academics and ultimately citizens to engage on these issues. In the end, we will only get the level of accountability that we are prepared to demand.

Whistle-Blowing

There is a need for multiple and even potentially redundant accountability mechanisms. One such fail-safe, one that the President's Review Group appointed in the wake of the Snowden revelations seems determined to shut down, is whistle-blowing. To be sure, whistle-blowing is a delicate subject, especially given Canada's vulnerable status as a net importer of intelligence and the recent memory of Jeffrey Delisle's criminal leaks that put at risk much Five

Eyes information. Nevertheless, there is a need for a more credible whistle-blowing mechanism than section 15 of the *Security of Information Act*.[97] This provision authorizes only a most limited form of whistle-blowing when a person with access to secret information has a reasonable belief that an offence has been committed. The whistle-blower must inform his or her civil service boss first, thus risking dismissal and prosecution. He or she can only inform SIRC or the CSE commissioner if he or she has not received a reasonable response from his or her boss. The CSE commissioner has never reported receiving a complaint from a potential whistle-blower.

If legal whistle-blowing is to be a realistic option, legislative reform is necessary. There needs to be real protection against prosecutions and perhaps a "single person and office"[98] such as a super SIRC to hear from whistle-blowers. The President's Review Group similarly recommended that an expanded civil liberties and privacy protection board have enhanced powers to hear from whistle-blowers.[99] In Canada, however, there is no parliamentary interest (even in Bills C-44 and C-51) in modernizing the *Security of Information Act* on whistle-blowing or other subjects. For example, Parliament has not even replaced an offence of the possession of secret information that was found by a trial judge in Ontario to violate the *Charter*.[100]

The impact of the WikiLeaks and Snowden leaks raises the uncomfortable question of the role of civil disobedience, or what Reg Whitaker aptly calls "guerilla accountability."[101] Although the Delisle leaks were embarrassingly low tech and done without good motives, the very same technology that empowers surveillance also empowers equally massive leaks. It took Daniel Ellsberg a year to sneak the seven thousand pages of the Pentagon Papers out of the Pentagon. Today, massive amounts of information can be downloaded and leaked in a matter of minutes.[102] The President's Review Group was well aware of this danger. It called for much tighter standards of access to secret information, with little apparent thought to whether its attack on the "need to share" could impede the quick flow of intelligence and the breaking down of walls that so many thought was so important after 9/11.[103]

To be sure, the Snowden leaks were unlawful. The robust debate about Mr. Snowden's fate is revealing. In some respects, it invokes Oren Gross's controversial post-9/11 proposal of an extra-legal approach to counterterrorism.[104] In other words, a failure to prosecute Snowden or even a light sentence would amount to a

form of ratification of his conduct. Future leakers, however, would not know for sure whether their leaks would be prosecuted or not. The idea that illegal leaks can be considered as a legitimate part of a system of accountability is an uncomfortable thought, but it cannot be ignored.

The Role of the Investigative Media

There could be no Edward Snowden without reporters such as Glenn Greenwald. This raises the precarious state of the traditional media today. Leaks publicized by the *New York Times*, *The Guardian*, and *der Spiegel* have a legitimacy (and a sense of responsibility about endangering individuals) that may not be present when they come from "some guy" with a computer and a blog. But the media itself is becoming more fragmented. Some question whether there will even be a mainstream media in the future. If there is not, governments may be able to dismiss dissent to surveillance and the security state as simply the musings of an extremist, radical, and disenfranchised fringe. Once again, the theme that we will ultimately get the accountability we deserve emerges with some force.

Conclusion

There are accountability gaps in all democracies, but Canada's accountability gap is particularly pronounced. Alone out of our Five Eyes partners, Canada still does not give any parliamentarians access to secret information. SIRC was state-of-the-art when it was created in 1984, but comparable Australian and British reviewers now are much closer to a whole-of-government mandate that is fit to review whole-of-government security. American Inspectors General have had more success than Canadian review bodies in conducting joint investigations.[105] The government abolished CSIS's Inspector General in 2012. The US Privacy and Civil Liberties Board and a similar one created in 2015 in the UK have a whole-of-government mandate. These developments suggest that review in Canada is becoming increasingly out of date and out of step with attempts in other democracies to plug post–9/11 accountability gaps. Bill C-51 and especially its *Security of Canada Information Sharing Act* will significantly expand Canada's already large accountability gap by its failure to match whole-of-government information sharing with effective whole-of-government review.

At the same time, Bill C-51 has resulted in increased public and political attention to review and oversight. Increased interest in parliamentary review will not, however, plug fundamental accountability gaps. Proposals for enhanced parliamentary review have been mild proposals for a statutory committee of parliamentarians who will be bound by Canada's strict official secrets legislation. The experience of other democracies suggests that legislators can have their hands tied when they are briefed into alarming secret programs. Parliamentarians may have difficulties navigating the legal and bureaucratic complexities of complex whole-of-government approaches to security, especially without dedicated staff. They will also face temptations to use security issues for partisan advantage. Even if some parliamentarians, especially in the unelected Senate, can rise above the fray and master the complex security environment, they will still remain part-time amateurs. To be sure, they can make contributions, but they are likely to be modest ones.

Enter the professionals. Both Bill C-44 and Bill C-51 will give specially designated Federal Court judges new roles in authorizing CSIS to conduct surveillance and engage in disruption and threat reduction in violation of Canadian and foreign laws, including the *Charter*. Many will be comforted by the prospect of a judge being on the case and the government's defence of both bills stresses this feature. Moreover, Justice Mosley's expert calling-out of CSIS for subcontracting surveillance to Five Eyes partners demonstrates the power of a judge scorned. At the same time, however, heroic efforts of judges only go so far. The judicial oversight offered in these bills will typically be in the form of a closed proceeding with only the government's lawyer present. Although judges will expect their orders to be obeyed, there are no provisions in the new warrant provisions for adversarial challenges or appeals. Once a judge has determined the extent that CSIS must break laws and contravene the *Charter*, that one decision will generally be the final word. Indeed, even criticism of the judgment may not be possible if the judgment must for operational reasons remain secret or heavily redacted. Review bodies will hopefully be able to see the classified reasons, but they may also understandably be reluctant to question judicial decisions.

Full-time professional executive watchdogs are critical to closing accountability gaps. Here, matters have gotten worse since the Arar Commission concluded in 2006 that Canada's silo-based, twentieth-century review structure was manifestly inadequate for

the post–9/11 whole-of-government approach to security. SIRC has struggled in the intervening years with personnel issues. After the Inspector General for CSIS was abolished in 2012, SIRC had to take on the important work of determining the legality of CSIS's conduct. The CSE commissioner has been quick but often defensive in responding to the Canadian aspects of the Snowden leaks. The proposed *Security of Canada Information Sharing Act* in Bill C-51 will considerably widen the accountability gap by allowing all government entities to share broadly defined security information with seventeen federal agencies and departments. When Bill C-51 is enacted, Canada's significant accountability gap will become an accountability chasm.

Although the government warns that increased review will be "needless red tape," the time has come to replace SIRC, the CSE commissioner, and others with a "super SIRC" that has jurisdiction to review all of the government's national security activities, including information sharing, under the proposed *Security of Canada Information Sharing Act*. A super SIRC should be creatively appointed and staffed. It could include elements of the quasi-judicial found in the CSE commissioner and elements of the tri-partisan found in SIRC. But more creativity will be required to command the confidence and engagement of a more diverse and fragmented public. A super SIRC needs not only a whole-of-government mandate but adequate resources, expertise, and staff to review the agencies and to engage with civil society.

Even if all of this happened, closing accountability gaps would remain an uphill battle. All branches of government and new and creative hybrid institutions must contribute, but so too must civil society, corporations (especially telecommunications companies), and the investigative media. A continued failure to close our growing accountability gap will leave both our rights and our security in increased jeopardy.

Acknowledgements

I thank Mel Cappe, Craig Forcese, and Wesley Wark for helpful and challenging comments on a much earlier draft of this chapter. I wish also to thank Mel Cappe for his enthusiastic support for increasing and enriching public debate about national security matters in Canada and his dedicated public service.

Notes

1. Canada, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works, 2006) at 456–58. The author was part of a research advisory committee for this report.
2. Four former prime ministers, as well as former members of the Security Intelligence Review Commission (SIRC) and Privacy Commissioners, signed a joint letter in February 2015 that noted that the government had not acted on the recommendations of the Arar Commission and stressing the need for "cross agency reviews." Jean Chrétien, Joe Clark, Paul Martin, & John Turner, "A Close Eye on Security Makes Canadians Safer," *Globe and Mail*, 19 February 2015.
3. Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Air India Flight 182: A Canadian Tragedy* (Ottawa: Public Works and Government Services Canada, 2010). The author was the director of research (legal studies) for the commission.
4. Bill C-51, *Anti-Terrorism Act*, 2015 1st reading, 30 January 2015, Part I, *Security of Canada Information Sharing Act*. The government's backgrounder stresses that the Privacy Commissioner will conduct whole-of-government review, even though the Privacy Commissioner indicated in a 2014 report that the office requires more legal powers with respect to security information sharing, including joint investigations and access to the Federal Court with respect to collection and disclosure of personal information. See Canada, Office of the Privacy Commissioner of Canada, *Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance* (Ottawa: Public Works and Government Services Canada, 2014). Bill C-51 does not contain the reforms suggested by the Privacy Commissioner.
5. Bill C-51 *Ibid*., Part 4. See also *Protecting Canadians from Terrorism Act* S.C. 2015 c.,9 (Bill C-44)
6. David Pugliese, "Government Knows Best, Says Conservative MP, No Need for More Oversight on Spy and Security Agencies," *Ottawa Citizen*, 1 February 2015; Aaron Wherry, "The Heart of Our Democracy in a Time of Terror," *Maclean's*, 5 February 2015, <http://www.macleans.ca/politics/the-heart-of-our-democracy-in-time-terror/>.
7. Hansard, 19 February 2015, per Hon. Peter Van Loan; Tonda MacCharles & Bruce Campion-Smith, "Stephen Harper Rejects Calls for More Oversight of New Spy Powers," *Toronto Star*, 19 February 2015.
8. *Protecting Canadians from Terrorism Act*, *supra* note 5.
9. In the matter of an application by X for a warrant pursuant to sections 12 and 21 of the *Canadian Security Intelligence Service Act* [2013] FC 1275, aff'd [2014] FCA 249 leave to SCC granted 5 February 2015.

10. For an argument that judges as unelected amateurs should defer to the state on security matters, see Adrian Vermeule & Eric Posner, *Terror in the Balance* (New York: Oxford, 2007).
11. US, The Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World* (Washington, DC, 2013).
12. See, for example, Office of the Communications Security Establishment Commissioner [CSEC Commissioner], *Annual Report 2005–2006* at 9–10 (Ottawa: Public Works and Government Services Canada, 2006); CSEC Commissioner, *Annual Report 2006–2007* at 2–3 (Ottawa: Public Works and Government Services Canada, 2007).
13. *Supra* note 11.
14. For my earlier conceptualization of social accountability, see Kent Roach, "Public Inquiries and Three Processes of Accountability," in *Accountability for Criminal Justice*, ed. Philip Stenning (Toronto: University of Toronto Press, 1995), 268–293.
15. David Cole, "Where Liberty Lies: Society and Individual Rights," (2011) 57 Wayne L. Rev. 1203.
16. For additional analysis of the distinction between efficacy and propriety based review, see Reg Whitaker & Stuart Farson, "Accountability in and for National Security," (2009) 15:9 IRPP Choices 1.
17. *Supra* note 1 at 499–503.
18. *Ibid.* at 456–58.
19. *Ibid.* at 458–63.
20. *Ibid.* at 500.
21. *Ibid.* at 467.
22. See generally Phillip Stenning, ed. *Accountability for Criminal Justice* (Toronto: University of Toronto Press, 1995).
23. For discussion of accountability gaps, including how public inquiries have had to be appointed with extraordinary jurisdiction to review the activities of all government officials in particular security areas, see Kent Roach, *The 9/11 Effect: Comparative Counter-Terrorism* (Cambridge: Cambridge University Press, 2011) at 455–59; Kent Roach, "Public Inquiries as an Attempt to Fill Accountability Gaps Left by Judicial and Legislative Review," in *Critical Debates on Counter-Terrorism Judicial Review*, eds. Davis & de Londras (Cambridge: Cambridge University Press, 2014) at 183ff.
24. *CSIS Act*, s. 34.
25. *National Defence Act*, s. 273.63.
26. *Supra* note 17 at 468.
27. Canada, Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Air India Flight 182: A Canadian Tragedy* (Ottawa: Public Works and Government Services Canada, 2010) vol. 3 at 1.

28. The government has provided a formal response to the report and issued a progress report but both documents are silent with respect to this critical recommendation about the enhanced role of the PM's national security advisor.
29. *Act to amend the RCMP Act* S.C. 2013, c. 18, ss. 45.4–45.43.
30. *Attorney General of Canada v. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar*, 2007, FC 766.
31. List of SIRC reviews under section 54 of the *CSIS Act*, 10 November 2014, <http://www.sirc-csars.gc.ca/opbapb/lsrlse-eng.html>.
32. Classified reports, 20 August 2014, <http://www.ocsec-bccst.gc.ca/ann-rpt/cr-rc_e.php>.
33. Justice Décary made this statement while at the same time correctly noting that "where CSEC and CSIS cooperate and conduct joint activities, my office and SIRC do not have an equivalent authority to conduct joint reviews." Canada, CSEC, *Annual Report 2012–2013* (Ottawa: Minister of Public Works and Government Services, 2012) at 5.
34. Pugliese, *supra* note 6.
35. *Ibid.*
36. Chris Hall, "CSIS Watchdog Agency Starved of Staff, Resources," *CBC News*, 20 February 2015, <http://www.cbc.ca/news/politics/csis-watchdog-agency-starved-of-staff-resources-1.2965276>.
37. Canada, Office of the Privacy Commissioner of Canada, *supra* note 4.
38. Kent Roach, "The Problems with the New CSIS Human Source Privilege in Bill C-44," (2014) 61 C.L.Q. 451.
39. *An Act to Establish the National Security Committee of Parliamentarians*, 2nd Sess., 41st Parl., 2013, cls. 10–11 (first reading 7 November 2013) Bill C-551.
40. *Ibid.* cl. 14.
41. Section 14(4) (c) of the bill encourages the minister not to disclose information to the committee if it was obtained from foreign states without even asking, as courts increasingly require, whether the foreign state would be prepared to amend any caveat restricting further disclosure of shared intelligence.
42. Bill C-622, 2nd Sess., 41st Parl., defeated on second reading, 5 November 2014.
43. *Supra* note 16 at 35.
44. Amy Zegart, *Eyes on Spies* (Stanford: Hoover Institution Press, 2011).
45. Bruce Ackerman, *Before the Next Attack* (New Haven, CT: Yale University Press, 2005); Stephen Schulhofer, "Oversight of National Security Activities in the United States," in *Secrecy, National Security and the Vindication of Constitutional Law*, eds. David Cole et al. (Cheltenham: Elgar, 2013) at 42.
46. Phillipe Lagassé, "Accountability for National Defence," (2010) 4 IRPP Study at 8-12. Lagassé conflates accountability and control when he

asserts that a stronger parliamentary committee could undermine the responsibility of the minister and the Cabinet for defence.

47. Canada, Office of the Privacy Commissioner of Canada, *supra* note 4 at 12.
48. *Supra* note 1 at 491.
49. *Ibid*. at 439.
50. *Charkaoui v. Canada*, [2007] 1 S.C.R. 350; *Charkaoui v. Canada* [2008] 2 S.C.R. 326; *Harkat v. Canada* 2014 SCC 37.
51. *Abdelrazik v. Canada*, [2009], F.C. 580.
52. [2013] FC 1275 at para. 117.
53. *Ibid*. at para. 110.
54. *Ibid*. at para. 115.
55. *Protecting Canadians from Terrorism Act* S.C. 2015 c. 9 adding s. 21(3.1) to the *CSIS Act*; Bill C-51, adding s. 21.1(4) to the *CSIS Act*.
56. Bill C-51, adding ss. 12.1(3) and 21.1 to the *CSIS Act*.
57. Bill C-51, adding s. 12.2 to the *CSIS Act*.
58. Laura Payton, "C-51 Confusion Abounds as Tories Rush Bill C-51 to Committee," *CBC News*, 20 February 2015, <http://www.cbc.ca/news/politics/c-51-confusion-abounds-as-tories-rush-anti-terrorism-bill-to-committee-1.2963569>.
59. *Atwal v. Canada*, (1987), 36 C.C.C. (3d) 16 (Fed.C.A.).
60. Privacy and Civil Liberties Oversight Board, R*eport on the Telephone Records Program Conducted under Section 215 of the USA Patriot Act and on the Operations of the Foreign Intelligence Surveillance Court*, 23 January 2014, <https://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf>.
61. Craig Forcese & Kent Roach, "Bill C-51 Backgrounder # 2: The Canadian Security Intelligence Service's Power to 'Reduce' Security Threats Through Conduct that May Violate the Law and Charter," *Social Science Research Network*, 12 February 2015, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2564272>. See also Kent Roach & Craig Forcese, "Legislating in Fearful and Politicized Times: The Limits of Bill C-51's Disruption Powers in Making Us Safer" in Edward Iacobucci and Stephen Toope, eds. *After the Paris Attacks: Responses in Canada, Europe and Around the Globe* (Toronto: University of Toronto Press, 2015).
62. Bill C-51, adding ss. 21.1 to the *CSIS Act*.
63. Human Rights Watch, *Preempting Justice: Counter-Terrorism Laws and Procedure in France* (New York: Human Rights Watch, 2008) at 14–18.
64. Application under s. 83.28 of the *Criminal Code*, [2004] 2 S.C.R. 248; Re *Vancouver Sun*, [2004] 2 S.C.R. 332.
65. Bill C-51, adding s. 12.1(2) to the *CSIS Act*.
66. Bill C-51, adding s. 12.2 to the *CSIS Act*.
67. MacCharles & Campion-Smith, *supra* note 7.

68. Greg Weston, "Other Spy Watchdogs Have Ties to the Oil Business," *CBC News*, 10 January 2014, <http://www.cbc.ca/news/politics/other-spy-watchdogs-have-ties-to-oil-business-1.2491093>.
69. SIRC, *Lifting the Shroud of Secrecy: Thirty Years of Security Intelligence Accountability, Annual Report 2013–2014* (Ottawa: Public Works and Government Services Canada, 2014), <http://www.sirc-csars.gc.ca/pdfs/ar_2013-2014-eng.pdf>.
70. "Statement by CSE Commissioner the Honourable Robert Décary," *Office of the Communications Security Establishment Commissioner*, 13 June 2013, <http://www.ocsec-bccst.gc.ca/media/pr/2013-06-14_e.php>.
71. *Ibid.*
72. *Supra* note 33 at 25.
73. *Ibid.*
74. Commissioner Décary announced, "It is well understood that Canadian federal law enforcement and security agencies may lawfully investigate Canadians. When these organizations request the assistance of CSEC, I verify that CSEC complies with any limitations imposed by law on the agency to which CSEC is providing assistance, for example, any conditions imposed by a judge in a warrant." *Supra* note 70. As discussed above, Justice Mosley's subsequent decision released in December 2013 found that the enlistment of Five Eyes partners to assist in the surveillance of Canadian citizens outside of Canada exceeded both the scope of his warrant and the limitations imposed in law on both CSIS and CSEC.
75. See, for example, CSEC Commissioner, *Annual Report 2005–2006* at 9–10; CSEC Commissioner, *Annual Report 2006–2007* at 2–3.
76. "Statement by CSE Commissioner the Honourable Jean-Pierre Plouffe re: January 30 CBC Story," *Office of the Communications Security Establishment Commissioner*, 31 January 2014, <http://ocsec-bccst.gc.ca/media/pr/2014-01-31_e.php>.
77. Greg Weston, "CSEC Used Airport Wi-Fi to Track Canadian Travellers: Edward Snowden Documents," *CBC News*, 31 January 2014, <http://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881>, quoting security experts Ron Deibert and Wesley Wark that the activities were outside CSEC's legal mandate.
78. The commissioner's mandate under section 273.63 is to review the legality of CSEC's activities and inform the minister of defence and the attorney general of Canada of activities that are not in compliance with the law.
79. Office of the Communications Security Establishment Commissioner, "Current Issues: Questions and Answers," n.d., <http://www.ocsec-bccst.gc.ca/new-neuf/faq_e.php>.
80. *National Defence Act*, RSC, 1985, c N-5, s. 273.64(2)(a).

81. For details on this ongoing litigation, see British Columbia Civil Liberties Association, "Stop Illegal Spying: Case Details," <https://bccla.org/stop-illegal-spying/protect-our-privacy-case-details/>.
82. Canada, Public Safety Canada, "Backgrounder on the Security of Canada Information Sharing Act," 30 January 2015, <http://news.gc.ca/web/article-en.do?nid=926879>.
83. Canada, Office of the Privacy Commissioner of Canada, *supra* note 4.
84. Kent Roach, "Illusory Accountability but Real Accountability Gaps," in *Putting the State on Trial*, eds. M. Beare et al. (Vancouver: University of British Columbia Press, 2015).
85. For more detail, see Craig Forcese & Kent Roach with Leah Sherriff, Bill C-51 Backgrounder #5, "Oversight and Review: Turning Accountability Gaps into Canyons?" *Social Science Research Network*, 27 February 2015, <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2571245>.
86. This would greatly expand SIRC's mandate in part because of the breadth of the government's proposed security predicate for the *Security of Canada Information Sharing Act*. For criticism of this broad category of activities that undermine the security of Canada, see Roach & Forcese "Backgrounder #3: Sharing of Information and Lost Lessons from the Maher Arar Experience," 16 February 2015, <http://antiterrorlaw.ca>.
87. The need to include former parliamentarians on a super SIRC, with the potential for conflicts of interest, might be less if a parliamentary committee with access to secret information was also created. Indeed, there seems to be a trend away from appointing former parliamentarians to serve on SIRC with none of the members as of April 2015 having served in elective office.
88. *R. v. Spencer*, 2014, SCC 43.
89. Canada, Office of the Privacy Commissioner of Canada, *supra* note 4 at 11, calling for better definition of terms in the CSEC enabling legislation.
90. See, for example, CSEC Commissioner, *Annual Report 2005–2006* at 9-10; CSEC Commissioner, *Annual Report 2006–2007* at 2–3.
91. Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated under s. 702 of the Foreign Intelligence Surveillance Act*, July 2014 at 146.
92. *Counter Terrorism and Security Act*, 2015, c. 6, ss. 42–43.
93. See Michael Geist, Chapter VIII.
94. Ronald Diebert, "Shutting the Backdoor: The Perils of National Security and Digital Surveillance Programs," Strategic Working Group Papers (October 2013): 8, <http://opencanada.org/wp-content/uploads/SL13CIC018-SSWGP-Deibert-v3.pdf>.
95. Campbell Clark, "New Poll Finds Terrorism Bill a Political Juggernaut," *The Globe and Mail*, 19 February 2015, <http://www.theglobeandmail.com/news/politics/new-poll-finds-harpers-anti-terror-

bill-is-a-political-juggernaut/article23067983/>. Since that poll, public support for Bill C-51 seems to have declined, but the government has proceeded with the legislation.

96. Jean Chrétien, Joe Clark, Paul Martin & John Turner, "A Close Eye on Security Makes Canadians Safer," *Globe and Mail*, 19 February 2015, <http://www.theglobeandmail.com/globe-debate/a-close-eye-on-security-makes-canadians-safer/article23069152/>.
97. R.S.C., 1985 c. O-5. CSE and CSIS but not other agencies that use secret intelligence are exempted from general whistle-blower protection in the *Public Servants Disclosure Protection Act*, S.C. 2005, c. 46 that might otherwise apply in cases where illegal conduct, such as intelligence including metadata, was used in a way to pose a risk to a person's life.
98. Wesley Wark, "Intelligence Requirements and Anti-Terrorism Legislation," in *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*, eds. Ronald Daniels et al. (Toronto: University of Toronto Press, 2001) at 291.
99. *Supra* note 11 at 198. The report, however, only devotes one paragraph to this proposal. In contrast, the report devotes twenty-five pages of detailed analysis and recommendations to the stopping of leaks. *Ibid.* at 233–58.
100. *O'Neill et al. v. The Attorney General of Canada*, (2006) 82 O.R.(3d) 241 (Sup Ct.).
101. See Reg Whitaker, Chapter VII.
102. Jesse Kline, "Knowledge, Power And Accountability: The Democratic Significance of WikiLeaks in the Digital Age," *National Post*, 30 September 2013, <http://news.nationalpost.com/2013/09/30/knowledge-power-and-accountability-the-democractic-significance-of-wikileaks-in-the-digital-age/>.
103. *Supra* note 11 at ch. 8.
104. Oren Gross, "Chaos and Rules," (2003) 112 *Yale Law Journal* 1011.
105. More on these comparative review mechanisms can be found in Forcese and Roach with Sherriff, *supra* note 85.

Page left blank intentionally