UNIVERSITY OF CALGARY

THE SCHOOL OF PUBLIC POLICY PUBLICATIONS

SPP Research Paper

Volume 13:12 May 2020

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

REVIEWING BILL C-59, *AN ACT RESPECTING NATIONAL SECURITY MATTERS 2017*: WHAT'S NEW, WHAT'S OUT, AND WHAT'S DIFFERENT FROM BILL C-51, *A NATIONAL SECURITY ACT 2015*?

Michael Nesbitt

SUMMARY

In 2015, Canada's national security law landscape received some long-overdue attention in the form of Bill C-51, the *Anti-Terrorism Act*. It was the culmination of a series of smaller initiatives that had brought attention to national security law in Canada, but also a direct response to two terrorist attacks that left two Canadians dead in October 2014. Bill C-51 did indeed reinvigorate discussions around national security law in Canada, but it became a lightning rod for criticism. Bill C-59, *An Act Respecting National Security Matters* 2017 was not passed until June 2019, but it was nevertheless a direct response to Bill C-51 and the criticisms it faced. Yet for the most part, Bill C-59 amended but did not repeal the important new powers, or even the most controversial ones, found in Bill C-51. Instead, Bill C-59 can be seen, in part, as a technical-legal bill that largely entrenched the powers first conceived of in Bill C-51 by putting them on firmer constitutional footing. But Bill C-59 was also much more than a series of legal/constitutional improvements: its legislative scope went much further afield from the Bill C-51 regime, amending the authorities of agencies –

http://dx.doi.org/10.11575/sppp.v13i0.69409 www.policyschool.ca

such as the Communications Security Establishment – that had been untouched by Bill C-51, while also greatly expanding national security oversight and review through the creation of important new bodies. The purpose of this paper is to compare these two important pieces of national security legislation with a view to explaining what these legislation reforms did, why the reforms were undertaken, and to identify the relative strengths and weaknesses of the most controversial of the reforms under each bill. The idea is to explain where Canada stands today, in the wake of this massive legislative overhaul. By identifying what has already been addressed, we can identify next steps and, in particular, where the focus of future legislative reforms in national security should be. Three recommendations flow from this conclusion. First, national security legislation must be reformed with greater consistency than in the past. Second, as an immediate priority, Canada must address its "intelligence-to-evidence" problem; that is, the system by which it converts – or fails to convert – raw intelligence into the sort of evidence usable by courts of law. Third, enforcement of Canada's national security laws must now take priority, in particular by prosecuting returning foreign fighters and far-right extremists where their activities meet the threshold of a terrorism offence, as well as terrorist financing, to a greater degree than Canada has seen to date.

INTRODUCTION:

The recent passage of Bill C-59, *An Act Respecting National Security Matters,*[1] represents a monumental transformation of Canada's national security landscape. Indeed, this is perhaps the largest and most important series of amendments since the CSIS act[2] created the Canadian Security Intelligence Service (CSIS) in 1984.

Bill C-59's amendments include replacing the CSIS oversight agency (the Security Intelligence Review Committee or SIRC*)* with the National Security and Intelligence Review Agency (NSIRA), which is empowered to review the activities not just of CSIS, but also matters of national security across a host of government departments.[3] Another amendment creates a new intelligence commissioner (IC) responsible for overseeing certain actions related to data collection by both CSIS and the Communications Security Establishment (CSE).[4] Other amendments include greatly expanding CSE's authorities and duties through its own legislation (CSE's mandate had previously been found in the *Department of National Defence* (DND) *Act*),[5] revising CSIS's powers and restrictions,[6] amending certain Criminal Code of Canada terrorism provisions[7] and beginning the process of unravelling the Kafkaesque quagmire of the no-fly list kids (#No-Fly List Kids n.d.; Zilio and Dickson 2019).[8]

Bill C-59 did not emerge out of the ether; its conception, though not all aspects of the bill, can be traced to 2015's Bill C-51, which became the *Anti-Terrorism Act* 2015[9] and put Canada's national security landscape in the public eye in a significant way. Bill C-51 was presented as a direct response to the two terrorist attacks of Oct. 20 and 22, 2014. The first was the murder of Patrice Vincent, a Canadian Armed Forces (CAF) soldier (Tucker and Frisk 2014); the second was the murder of Cpl. Nathan Cirillo, another CAF member who was guarding the Ottawa War Memorial (Tucker 2014). As responsive legislation, Bill C-51 was passed in short order (within eight months after the October attacks[10]) and, perhaps not surprisingly, the process and the end product created a good deal of public

---

1 *National Security Act,* 2017*,* S.C. 2019, ch. 13. Available at https://www.parl.ca/DocumentViewer/en/42-1/bill/C-59/royal-assent The bill was given Royal Assent on June 21, 2019, making it an Act of Parliament [Bill C-59]. See Canada. Parliament, *Debates of the Senate*, 42nd Parl., 1st Sess., vol. 150, no. 308 (June 21, 2019), 8845.

2 *Canadian Security Intelligence Service Act*, R.S.C. 1985, ch. C-23 [CSIS act].

3 *National Security and Intelligence Review Agency Act,* S.C. 2019, ch. 13, s. 8 (s. 2 of Bill C-59) [NSIRA act].

4 *Intelligence Commissioner Act,* S.C. 2019, ch. 13, s. 12 (s. 50 of Bill C-59) [IC act].

5 *Communications Security Establishment Act*, S.C. 2019, ch. 13 (s. 76 of Bill C-59) [CSE act].

6 Bill C-59, ss. 92-109.

7 Ibid., ss. 140-150.

8 Ibid., ss. 127-139.

9 *Anti-Terrorism Act,* 2015, SC 2015, ch. 20 [Bill C-51].

10 See Bill C-51.

controversy (Forcese and Roach 2015b).[11] Indeed, the controversy over Bill C-51 become an election issue in 2015, with the Conservative party (2015, 79) campaigning on the amendments that C-51 ushered in and its tough response to the Parliament Hill terror attack. The Liberal government (2015, 53) vaguely pledged at the time to revisit the bill and its more controversial provisions. The Liberals also promised to consult Canadians broadly about changes to national security policy and to create parliamentary capacity to scrutinize the work of security agencies (both of which they did).

This paper offers an overview and comparison of the major amendments found in both bills. Through this comparison, Bill C-59 is seen as more comprehensive in terms of the sheer scope of the amendments to Canada's national security landscape, but it is also more robust in that it generally accords better with Canadian legal – and particularly constitutional – obligations. This should come as no surprise because Bill C-59 is intended to be an update and improvement. In significant ways, it builds on the existing architecture created by Bill C-51. As an example, Bill C-59 does not undo the ever-controversial C-51 disruptive powers granted (under legal pre-conditions) to CSIS to act to limit *Charter* rights and other laws when disrupting national security threats, nor does it create a wholly new disruption regime. Rather, the existing legal infrastructure built by Bill C-51 – and the general legal justifications used to support the regime – are broadly reproduced in Bill C-59, though with added detail and specificity to ensure that those justifications pass constitutional muster. In this way, Bill C-59 did not so much undo Bill C-51 as expand it both in scope and legal viability. It took a nascent structure for CSIS's disruptive powers, or for information sharing between government agencies, and built on these, while addressing whole new (long overdue) issues in other areas of national security. In this way, much of C-51 survives post-C-59, though now in a legal form that better (though not necessarily completely) ensures its constitutionality. Bill C-59's primary contribution is, then, really in: (1) its legal innovations and (2) its new amendments, particularly those expanding CSE's powers and creating a system of national security review and oversight bodies (the creation of NSIRA and the IC).[12]

However one views a comparison between these two national security bills, surely most can agree that Canada's half-decade-long focus on national security law and practice has left the country in 2020 in a much better place than it was before, even as the threat environment expands and becomes more complicated. Post-Bill C-59, Canada's security agencies have expanded powers and authorities to act with greater certainty and efficacy (and protections) in dealing with today's threat environment. Their powers are better understood both inside the agencies and without, which builds transparency into their processes and with it public trust. Their authorities to act come with greater legal and operational clarity, the lack of which can contribute to operational paralysis. At the same time, Canadian civil liberties are also arguably better protected than they were pre-Bill C-59.

---

11 The legal criticisms in particular were far-reaching and led by professors Craig Forcese and Kent Roach.

12 One might reasonably add the long overdue datasets collection regime for CSIS as well. See Bill C-59, ss. 92-97.

This paper will proceed by first offering an overview of Bill C-51, its contents and its primary controversies. It then examines Bill C-59 as a response and replacement to Bill C-51. In the end, we see that the two bills were drafted under very different circumstances and political leadership, but they share the serious aspiration of improving a long-stagnant national security legal landscape. Yet Canada must not rest on its laurels; future governments have much work to do. No matter the sea change ushered in by Bill C-59 and C-51 before it, no end is in sight. To respond to the pace and progress of technology and the tactics of Canadian adversaries – whether terrorists or powerful foreign nation-states – Canadian national security agencies cannot continue to operate with antiquated legislation, revisited sparingly and only after serious attacks have already taken place. Responsible future governments will have to continue to monitor vigilantly national security law and practice, and update legislation in a much more timely fashion. This paper will thus end with several modest recommendations for legislative consideration starting as early as 2020.

OVERVIEW OF BILL C-51 AND THE CONTROVERSIES

In 2015, the Conservative government enacted Bill C-51, which became the *Anti-Terror Act.* Bill C-51 was not only an initial foray into updating an antiquated national security landscape, it was also a political and legal response to the deaths of two CAF members in the Parliament Hill (Tucker 2014) and Saint-Jean-sur-Richelieu terrorist ramming (Tucker and Frisk 2014) attacks. The response was swift: Bill C-51 was introduced on Jan. 30, 2015[13] and received royal assent on June 18, 2015.[14] Initially, there was great support for some legislative action because of the demand for a response to the killings of Cirillo and Vincent, and because Canada's national security landscape had largely been ignored despite numerous commissions of inquiry (Air India 2010, 1: 195-196; Almalki 2008, 12; Arar 2006, 364-369)[15] recommending serious changes to bring us up to date with our Five Eyes allies and international practice.

Although Bill C-51 kicked off a long overdue process of parliamentary review of national security legislation, it was ultimately passed with little public or expert consultation and limited committee debate, and it suffered the consequences. It created a series of authorities that were arguably unconstitutional and thus deemed ultimately unusable (e.g., the new CSIS disruptive powers) or even legally incomprehensible (the new Criminal Code offence of advocating terrorism[16]). This meant that regardless of best intentions, the practical results would necessarily be limited.

---

13 Canada. Parliament, *House of Commons Debates*, 41st Parl., 2nd Sess., vol .147, no. 166, Jan. 30, 2015.

14 Bill C-51.

15 As two small examples, the Arar inquiry recommended better information sharing and co-ordination and that the RCMP update its training. The Air India COI recommended modernizing the CSIS act. The Almalki report is less overt in its recommendations, though it did find many instances of deficient conduct, including a failure of communication between CSIS and Foreign Affairs.

16 For an excellent review of the legal problems associated with the "advocating terrorism" provision in Bill C-51, see Craig Forcese and Kent Roach, *False Security: The Radicalization of Canadian Anti-Terrorism*, 329-357.

The process of negotiating national security legal updates also opened a can of worms. If reforms were in the offing, then the expectation was that the long-standing national security commission of inquiry recommendations would be taken seriously, and that new governmental powers might be offset by civil liberty protections and new review and oversight bodies. This review and oversight was not recommended purely for civil libertarian purposes or to check the powers of the security agencies. Post-9/11 the Americans had instituted a series of reforms aimed at ensuring better information sharing among government departments (9/11 Commission 2004, 417), better oversight to ensure not just propriety but more efficacious and responsive operations of national security actors, and in particular better co-operation among agencies (9/11 Commission 2004, 411).[17] Canada had fallen behind and, in some cases, out of touch with its Five Eyes allies. (For example, it was the only country without a parliamentary review body, an omission that was not remedied until 2017 by the *National Security and Intelligence Committee of Parliamentarians Act.*[18])

Furthermore, there was a desperate need to update the national security authorities associated with Canadian agencies' technical (online and data) capacities. Previous major national security law initiatives dated back to the passage of the *Anti-Terrorism Act* 2001, which created the Criminal Code terrorism offences that we have today and, before that, to 1984, when the CSIS act was passed and CSIS came into being as a separate agency independent from the RCMP. In between, there was notoriously little movement. As a result, a whole host of national security laws and authorities had become stale. Almost certainly foremost among these was the CSE mandate, which left the agency reliant on extraordinarily limited authority to conduct electronic surveillance in an age where technology and national security practice were evolving daily.

Perhaps then, not surprisingly, the first and in some ways most salient criticism of Bill C-51 was what it did not do. It did not take seriously previous commission-of-inquiry recommendations related to the national security space; it did little to offer reforms like those in the U.S. and among its Five Eyes partners. While it offered expansive new powers for CSIS, it did so without corollary amendments to an antiquated review and oversight regime, which again was not merely a matter of legality but operational efficacy. (A failure to review the efficacy of existing procedures, to share information and to co-operate were all seen as contributing to intelligence failures around the globe; Canada surely was not the exception). The argument is not that the bill should, or could, have done everything. Rather, the point is that it ignored some of the most pressing issues (updates of CSE, national security review) while giving expansive new powers without the corollary legal protections.

So what did Bill C-51 do? First, it finally addressed a long-standing deficit in Canadian information-sharing regimes, in particular how Canadian agencies shared information within government, as between each other. Second and third, it introduced the *Secure Air Travel Act* and made amendments to the Criminal Code*,* introducing in the latter case

---

17 Enacted by the *Intelligence Reform and Terrorism Prevention Act* 2004, 50 USC 403-1 § 102A (2004).

18 S.C. 2017, ch. 15 (Assented to July 22, 2017).

several reforms, including a new advocating-terrorism offence. Last, Bill C-51 gave CSIS disruptive powers for the first time, allowing it to act kinetically to counter threats to national security. These initiatives are discussed below.

Security of Canada Information Sharing Act

The 9/11 Commission Report (2004, 352) and Canada's Air India bombing report (Air India 2010, 26) both recognized the importance of improved information sharing within the intelligence community, and the threat of failure to adequately share intelligence. Bill C-51 introduced the *Security of Canada Information Sharing Act* (SCISA) to address the culture of siloed investigations and information handling in Canada.

SCISA was a laudable initiative in that it hit on a recognized problem – not enough information sharing among security agencies – but it was replete with technical problems.[19] For example, SCISA's application to all activities "undermining the security" of Canada was defined much more broadly than its concomitant definition in the CSIS act.[20] It was argued at the time that the drafting could include powers to share information about "unlawful protests", which could securitize not just gatherings of terrorists groups but any protest that might run afoul of a bylaw (for example, where one protester or more were trespassing).

Moreover, SCISA ran up against a potential conflict with the *Privacy Act21* provisions to limit information sharing. SCISA promoted (but did not mandate) information sharing, while the *Privacy Act* limited some types of information sharing. The relationship between the two acts, and particularly which trumped which in the case of conflict, was legally uncertain.

Thus, SCISA's practical benefit was uncertain. Government departments could already share information pre-SCISA, except where there was an explicit prohibition on such information sharing, and there already existed a plethora of authorities and prohibitions to such information sharing (for example, in the *Privacy Act*). SCISA was then superimposed over these prohibitions with little detail as to how it would compel or allow disclosure. When confusion such as this reigns, one of two things happens. First, either all information is shared, which is bad for civil liberties because not all information should be shared. It's also bad for national security because when all information is critical, none of it is. Second, bureaucrats administering the provision will take an understandably cautious approach, knowing that there is no obligation to share information but, if shared, there might be legal repercussions if that information is deemed to have been shared contrary to other laws. A 2017 report by the privacy commissioner seemed to indicate that the latter eventuality was indeed coming to pass: there were astonishingly few disclosures over SCISA's first

---

19 For an excellent review of the technical-legal problems, see Craig Forcese and Kent Roach, "Bill C-51 Backgrounder #3: Sharing Information and Lost Lessons from the Maher Arar Experience," Feb. 16, 2015. Available at www.ssrn.com/abstract=2565886 .

20 CSIS act, s. 2.

21 *Privacy Act*, RSC 1985, ch. P-21.

year (Privacy Commissioner 2017).[22] In other words, there was real worry that while SCISA was laudable in its aspirations, they were not bearing fruit.

In the end, the idea of SCISA was nevertheless vital. A big part of this amendment was about encouraging a slow culture shift toward more effective information sharing between federal agencies, and that alone was extremely important. However, as noted, the technical implementation left a lot to be desired.

Secure Air Travel Act

Bill C-51 also created the *Secure Air Travel Act.*[23] This act modified the Passenger Protect Program and allowed (and still allows) for the creation of a list of people whom the minister believes, on reasonable grounds, will commit an act threatening transport security or may commit an act of terrorism.[24] Air carriers such as Air Canada are then required to impose additional screening on passengers whose names appear on the list.[25] Initial coverage of C-51 largely focused on other topics, with little said about the *Secure Air Travel Act* (Gadzo 2016; Macleod 2015). Then, around January 2016, reports of extensive additional screening for false-positives on the no-fly list – some of them young children – started to emerge (Elghawaby 2016).[26] The result led eventually to the so-called "no-fly list kids", a quagmire where, according to the group, up to 100,000 people and many children were wrongly flagged for additional, unnecessary screening (#NoFlyListKids n.d.).

Criminal Code Amendments and the Advocating-Terrorism Offence

Conversely, Bill C-51's amendments to the Criminal Code began as a major controversy and then took a backseat to the no-fly list and other controversies.[27] Most prominent among these[28] criminal amendments was the introduction of section 83.221 to the

---

22 The report found 118 SCISA disclosures, with only 97 of them acknowledged as being received. Aside from the low number, the quality of the disclosures was also suspect. For instance, in several cases information about family members of investigations was disclosed where "there was no evidence that such information was relevant to the jurisdiction or responsibilities of the recipient institution in respect of an activity that would undermine the security of Canada".

23 *Secure Travel Act,* SC 2015, ch. 20, s. 11.

24 Ibid., ch. 20, s. 11, s. 8. For background on the *Secure Air Travel Act*, see "Understanding Bill C-51: The Anti-Terrorism Act, 2015," Canadian Civil Liberties Association, May 19, 2015. Available at www.ccla.org/understanding-bill-c-51-the-anti-terrorism-act-2015/ Accessed July 2019.

25 *Secure Travel Act,* Ibid., s. 21.

26 The list contained very little personal information, often including only a person's name, meaning that people as young as six who shared names with listed persons were flagged as potential threats.

27 It should be noted that only one new offence was introduced in 2015 because, only two years or so earlier, the Conservative government passed the *Combating Terrorism Act*, SC 2013, ch. 9 [CTA]. It introduced a host of new criminal offences to the Criminal Code, including: leaving Canada to participate in terrorism – s. 83.181 (s. 6 of the CTA); leaving Canada to facilitate terrorism – s. 83.191 (s. 7 of the CTA); leaving Canada to commit offence for a terrorist group – s. 83.201 (s. 8 of the CTA) and leaving Canada to commit terrorist activity – s. 83.202 (s. 8 of the CTA).

28 Bill C-51 also introduced a new "warrant of seizure" – s. 83.222 (s. 16 of Bill C-51); and "order to computer system's custodian" – see Criminal Code, RSC 1985, ch. C-46 at s. 83.223 (ss. 16 & 35 of Bill C-51).

Criminal Code: "Advocating or promoting the commission of terrorism offences".[29] The new offence provided the following:

> **83.221** (1) Every person who, by communicating statements, knowingly advocates or promotes the commission of terrorism offences in general – other than an offence under this section – while knowing that any of those offences will be committed or being reckless as to whether any of those offences may be committed, as a result of such communication, is guilty of an *indictable* offence and is liable to imprisonment for a term of not more than five years.[30]

This "advocating" offence was based to a large extent on both a similar Australian advocating-terrorism offence as well as the related Canadian criminal offences of advocating genocide and the wilful promotion of hatred (Forcese and Roach 2015a, b).[31] Moreover, the United Kingdom had introduced a broader terrorist propaganda offence to counter what was viewed as the proliferation of advocates encouraging others toward terrorist (primarily Islamist extremist) ends (Coudhury and Fenwick 2011). The idea to amend the Canadian Criminal Code was thus consistent with what was viewed among at least several allied countries as a gap in their legislation, the idea being that the similar absence of such a criminal offence in Canadian legislation also meant that Canada had a gap to fill.

But, again, the execution came under attack, and the need for the new offence was questioned in the Canadian context (Forcese and Roach 2015a, b). Professors Craig Forcese and Kent Roach (2015a, 1), were the two most prominent critics of Bill 15 and they summarized their concern thus: "The new offence is broader than the offences on which it appears to be modeled, including Canadian offences of advocating under-age sex or genocide or willful promotion of hatred. It is also broader than the Australian offence of advocating terrorism, even though Australia does not have a constitutional bill of rights."

Moreover, the Canadian language made it a crime to advocate "terrorism offences in general", and while "terrorism offences" are explicitly defined in the Criminal Code, nobody knew what was added by the words "in general". More to the point, it was difficult to reconcile the goal of the new law with what it could reasonably hope to achieve and remain constitutionally valid. It is already an offence to counsel any crime in the Criminal Code, so the advocating offence was either redundant or offered something that counselling would not. The most obvious additional benefit was that while counselling applies to all offences, the new advocacy offence only applied to "terrorist offences in general", which were somehow different – and presumably broader – than

---

29 Ibid., s. 83.221.

30 Ibid., s. 83.221 as it appeared on June 20, 2019; *Anti-Terrorism Act* 2015, SC 2015, ch. 20, s. 16. Australia did add an advocacy offence in 2005: see Kent Roach, "A Comparison of Australian and Canadian Anti-Terrorism Laws," 30:1 *University of New South Wales Law Journal* 53 (2007), 82. See also Canada. Library of Parliament, *Legislative Summary of Bill C-51* (Ottawa: Library of Parliament, June 19, 2015), publication no. 41-2-C51-E. Available at www.lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/412C51E , which references that Australia, France and the U.K. had offences for "glorification of terrorism". Accessed July 2019.

31 For the criminal offences, see Criminal Code, ss. 318-319.

just terrorism offences. But if the latter interpretation was followed, then the scope of the advocacy offence was unknowably broad and seemingly unconstrained, including by the very "defences" that had been explicitly included in Canada's hate speech law to ensure its constitutionality, such as exceptions for art, honestly held religious belief, or even for lawyers who might be defending an accused terrorist.[32]

In criminal law, as with law in general, such uncertainty and unnecessary open-endedness can be a dangerous thing and the provision's language as a whole was put under the microscope. The controversy ultimately died down. The new advocacy speech crime was never charged and Bill C-59 ultimately kept it on the books, tweaking it by making clear that it was indeed a counselling offence and taking steps such as removing the words "in general". [33]

CSIS's New "Kinetic" Authority to Disrupt Threats to National Security in "Limitation" of the Law and Charter

Finally, perhaps the most controversial aspect of Bill C-51 was that for the first time, it gave CSIS the authority to "take measures, within or outside Canada" to disrupt "threats to the security of Canada", which is broadly defined.[34] The disruptive powers went well beyond those enjoyed by Canadian police, and included authority to limit any *Charter* right or Canadian law.[35] The only concrete limitation to such powers was that they not be exercised so as to cause death or bodily harm, violate sexual integrity or wilfully obstruct

---

32 Hate speech crimes have specifically carved out defences for demonstrably true statements, religious opinions, public interest or messages pointing out hate speech for removal, see Criminal Code, s. 319(1)(c). The Supreme Court placed considerable importance on these defences when it upheld the constitutionality of Canada's hate crime laws in *R. v. Keegstra* [1990] 3 S.C.R. 697. Available at https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/695/index.do

33 Bill C-51 inserted section 83.3 to the Criminal Code, which, along with several other provisions, included the capacity to remove "speech" from the internet under certain circumstances. See Criminal Code, s. 83.3. Moreover, Bill C-51 also introduced to the Criminal Code s. 810.011 – the terrorist peace bond. These peace bonds can be imposed for one year, or up to five years if the suspect has a previous terrorism conviction. Finally, Bill C-51 lowered the threshold for issuing a peace bond from a reasonable belief that the suspect "will" commit a terrorist offence to a belief that they "may" commit one. This might seem a minor amendment, but there was significant pushback at the time, particularly from the legal and civil liberties communities. For example, the International Civil Liberties Monitoring Group (n.d.) had this to say about the changes: "The Anti-terrorism Act of 2015 (Bill C-51) lowered the existing thresholds for peace bonds (section 810.011) and preventive arrest (section 83.3) and lengthened the amount of time someone can be held without being charged, while suggesting to judges a new range of conditions … C-51 substantially broadens the state's ability to control an individual's liberty without any criminal charge or conviction, and with minimal evidence of any criminal plan or intention by lowering the threshold for a preventive arrest from 'will commit' a crime to 'may commit' a crime." Of course, others, including law enforcement, saw a need for the amendments, in particular to ensure another tool in the law enforcement basket to fight against terrorism, which can be notoriously tricky to pre-empt, particularly when contemplating a determined adversary.

34 CSIS act, s. 12.1 as it appeared on June 17, 2019. Threats to the security of Canada are defined in section 2 of the CSIS act as: espionage, sabotage, foreign influence, violence for political, religious or ideological purposes, or activities aimed at violent overthrow of the government. There is an exemption for lawful protest and dissent, unless done in conjunction with the other activities.

35 Ibid.

justice.[36] There was also a requirement that, before exercising such powers, CSIS must assure itself that its actions were "reasonable and proportional in the circumstances".[37]

This new disruptive power was controversial primarily for two reasons. First, the reason CSIS did not have such powers in the first place was intentional. After it became public that the RCMP had perpetrated a series of unlawful activities in the 1970s to counter the FLQ terrorist threat –prominent among these actions being the burning of a barn to break up a gathering inside – the McDonald Commission recommended the creation of what would become CSIS (Sallot 2006). The commission also recommended that the physical powers to arrest and disrupt be kept in the hands of the police and exercised separately from intelligence-gathering authorities needed to keep an eye on threats to Canada's security. The McDonald Commission's recommendation was implemented when CSIS was subsequently formed in 1984, and CSIS was left without the power to physically disrupt threats. As a result, Bill C-51's about-face on that decision was bound to attract public scrutiny, particularly coming as it did after little public justification, consultation or discussion.

At the same time, the government's (and CSIS's) argument was also compelling: Times were changing along with the terrorist threat and, with technological and tactical advances of various threat actors, CSIS too needed additional powers to keep Canadians safe. There was never a robust discussion about what specifically had changed and why those changes necessitated these new disruptive powers for CSIS, as opposed to new authority for the RCMP coupled with more information-sharing permissions and protections between the agencies. Certainly, a more robust discussion would have been preferable, if for no other reason than that such a discussion leads to tailored legislation, which is more likely to withstand constitutional scrutiny. But, again, the general point was largely well taken. Thus, in the end, it was really the scope of CSIS's new powers – and their lack of clear legal limitations in all but the most egregious of circumstances –rather than the power to act disruptively *per se,* that garnered most of the attention.

That brings us to the second controversy surrounding Bill C-51's disruptive regime – the criticism that had more legs. This controversy was about the legality of the disruptive powers scheme and its capacity to withstand constitutional challenge and properly protect civil liberties.

The first check on CSIS's new authority was the requirement that its actions in limitation of a *Charter* right be proportional to the threat it was countering and that those disruptive actions were necessary in the context. These were primarily internal checks in that CSIS had to satisfy itself of these requirements, at least in the first instance. The second set of checks pertained to the scope of CSIS activities that might be undertaken in limitation of a *Charter* right: CSIS could take any action so long as it did not cause bodily harm or death, intentionally obstruct justice or "violate the sexual integrity of an individual", all presumably actions in which CSIS had no interest in engaging.[38]

---

36 Ibid., s. 12.2.

37 Ibid., s. 12.1.

38 CSIS act, s. 12.2.

Such a broad granting of power coupled with limited proscriptions or boundaries contributed to a serious constitutional flaw in the regime, which I have succinctly described before:[39]

> Generally speaking, the government cannot simply give itself such broad powers to breach any constitutional right with any action and very few legal limits, and then claim that all such actions undertaken under that power are legally authorized … Put another way, we have the Constitution's "notwithstanding clause," section 33 of the *Charter,* for a reason. If the government wishes to broadly exempt itself from the *Charter,* it should resort to that clause, not do an end-around by enacting legislation purporting to give itself [or perhaps better said, a judge] the unrestrained power to bypass the *Charter* (Nesbitt 2015).

Bill C-51 seemingly expected this line of critique and addressed it by creating a further, important limitation on CSIS's actions: it could not undertake disruptive activity in violation of the *Charter* without first seeking a warrant authorization from the Federal Court.[40] In this way, it was not the government legislating any *Charter* breach, but rather the government legislating that a judge could authorize any *Charter* breach. The judiciary then constrained disruptive power and any *Charter* breaches, just as our system demands.

To explain why this innovative legal structure was sound law and policy, a parallel was drawn to the police warrant regime. In short, the argument goes, section 8 of the *Charter* protects us all against "unreasonable" search and seizure by the state. In everyday police practice, police must (usually) get a warrant authorized by a judge before searching a home, for example. It was then implied that the Criminal Code's various warrant regimes were a parallel example of the government legislating authority for a judge to authorize a *Charter* breach. What is legal in one situation – police search warrants, for example – surely must be legal in another situation – CSIS disruption warrants.

However, the parallel between the section 8 process as applied to police actions and CSIS actions under the new disruptive regime was poorly drawn. The warrant authorization in the section 8 context is merely a process to affirm that the proposed search by the police is not "unreasonable". Remember, section 8 of the *Charter* only protects against "unreasonable" searches and seizures. The warrant authorization in the police context thus confirms the reasonableness of the proposed search; it definitively does not pre-emptively authorize a *Charter* breach. It does quite the opposite by ensuring that there is no *Charter* breach in the first place, before police take action, thus allowing police to act with a judicial assurance that they are in accordance with the *Charter*. The CSIS procedures, by contrast, ask the specially appointed Federal Court judge to pre-authorize any *Charter* breach, including of *Charter* rights that are not qualified in the way spelled out in section 8. Judicial pre-authorizations of *Charter* breaches are not how the *Charter* (or the judiciary) works. Such a process turns a judge into the legislature, determining

---

39 For a brief overview of other legal concerns, see Craig Forcese and Kent Roach, "Righting Security: A Contextual and Critical Analysis and Response to Canada's 2016 National Security Green Paper," *Canadian Yearbook of Human Rights*, no. 1.1 (2015), 72-73. Available at www.hri.ca/wp-content/uploads/2017/10/ottawau_canadianyearbookofhumanrights_vol1_2015.pdf Accessed September 2019.

40 CSIS act, s. 21.1.

what actions can be taken when, and with what limitations to breach any law or *Charter* right, in addition to the judge of that situation.

The regime thus looked more like an authorization for a judicial notwithstanding clause, where a judge is able to pronounce at will when *Charter* rights could be violated. Of course, Canada does have a process that allows for *Charter*-infringing behaviour. Section 1 of the *Charter* recognizes that various rights and freedoms are "subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society".[41] That section 1 process does not amount to an open-ended invitation to legislate judicial authority to breach any *Charter* right in whatever circumstances the reviewing judge sees fit. Rather, it requires, among other things, that the law be precise (not vague and open-ended, as Bill C-51's language was), that its limits are clearly defined, that the legislature demonstrably justify the specific rights limitations and ensure that the authorized state conduct is "minimally impairing" on those rights.[42]

Even if the above regime could meet a section 1 challenge, and that seems highly unlikely, the regime nevertheless did not contemplate how such a section 1 *Charter* challenge – needed to uphold the legislation – could ever take place. This brings us to the final concern, which is that the whole process was to take place in secret with only government lawyers present. This is exactly how police warrants are authorized, but again that broad similarity is where the parallels end. First, police warrants are executed so as to collect evidence for the purpose of making an arrest. The individual will then be charged and the warrant will be challenged in open court, or at least a defence lawyer will take a long look at doing so. In the CSIS context, no defence lawyer will ever have the capacity to challenge the basis or execution of the warrant. Moreover, problems regularly arise in the execution of a warrant, perhaps because of police malfeasance, but much more often because of mistakes, misunderstandings or because the situation demands that decisions be made. The open-court process protects against wrongdoing, whether intentional or by mistake, in the execution of a warrant; it does so by offering potential remedies, such as the possibility that a search warrant, and thus perhaps a criminal case, be thrown out. But the CSIS context is completely different. There will be no arrest; in fact, in many cases the intention will be a covert operation that never comes to light, and thus there will be no capacity to challenge the warrant or its subsequent execution. Indeed, under the Bill C-51 scheme, judicial oversight of the process stops when a judge authorizes the CSIS warrant. Finally, the Bill C-51 legislation explicitly contemplates the limitation of *Charter* rights by CSIS which, if one is justifying the regime by reference to section 1 of the *Charter,* then one would expect to see the opportunity for such a *Charter* challenge both to the regime and to specific operations that purport to limit *Charter* rights. However, if there is nobody to challenge the warrant then no proper section 1 challenge can take place, making it difficult to see how a *Charter* infringement could be justified.

---

41 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act* 1982, being Schedule B to the *Canada Act* 1982 (U.K.), 1982, ch. 11, s. 1.

42 For an easy-to-read review of the legal test needed to justify a *Charter* rights limit, see: Canada, Department of Justice, *Charterpedia.* Available at https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art1.html Accessed September 2019.

In this way, the legal protections associated with the police warrant process were emptied of their substantive content when enacted in the CSIS context: The warrant authorizing a *Charter* breach would never be challenged in an adversarial way; there was no party available to appeal the decision to ensure its propriety, the quality of the decision would never be tested in open court, and so on. As a result, CSIS never used its Bill C-51 powers of disruption in limitation of *Charter* rights until Bill C-59 updated the regime.

This is a good opportunity to turn to Bill C-59 to see what exactly it did and whether it responded successfully to all or some of the concerns levied at Bill C-51.

OVERVIEW OF BILL C-59: *AN ACT RESPECTING NATIONAL SECURITY MATTERS*

The debate around Bill C-51, and the broader debate about how to modernize Canada's national security landscape, came to a head in the 2015 federal election. The Liberals (2015, 53) promised to repeal the "problematic elements of C-51" and introduce new legislation, though the specifics of that promise, including what precisely was problematic and/or would be repealed, were never clear during the electoral campaign. What was clear was that, unlike the NDP (2015, 42), the Liberals would not repeal Bill C-51 in its entirety and would take a close look at how to amend, rather than fully redo, the legislation. As noted, they also promised (and delivered on) a broad consultation process with Canadians about changes to national security policy and to create a parliamentary capacity to review security agencies. By contrast, the Conservatives (2015, 79) made their support for Bill C-51 a policy plank and they promised to go a step further and introduce tough new national security legislation if elected. The election outcome would thus decide the fate of Bill C-51.

With the Liberal victory, two things were clear: Bill C-51 would not be repealed, but its provisions would certainly be amended in some way and the scope of those amendments would have to be clarified. The Liberals engaged in an extensive consultation process to identify the scope and nature of any amendments, starting with the issuance of a green paper on Canada's national security framework (PSEP 2016). The House of Commons Standing Committee on Public Safety and National Security also toured Canada to discuss the framework. The result was Bill C-59, *An Act Respecting National Security Matters*, which was a combination of reforms recommended after extensive public and expert consultations and a series of amendments that were never signalled or discussed publicly, including the reforms to CSE and the creation of an IC to oversee and review its functions.

Bill C-59 was granted Royal Assent on June 21, 2019, after over two years in hearings, almost four years to the day after C-51 was passed.[43] The act has 10 parts, many offering amendments to provisions of Bill C-51, discussed above, and many others creating new agencies or legal frameworks. For example, part 1.1 (tacked on late in the Bill C-59 process, after it was introduced to Parliament) is called "Avoiding Complicity in

43 Bill C-59.

Mistreatment of Foreign Entities". It requires that relevant government departments[44] issue public[45] directions on how they deal with information sharing with foreign governments. The impetus was the Arar case and the problems of information sharing identified by the Arar commission of inquiry (2006).[46] By contrast, part 5 of Bill C-59 revises the *Security of Canada Information Sharing [*now *Disclosure] Act,* introduced by Bill C-51, and confronts some of the problems associated with the creation of SCISA. Part 6 is entitled the *Secure Air Travel Act*, and its purpose is mainly to offer a technical fix to the Kafkaesque situation in which the no-fly list kids have found themselves.[47] These were each important initiatives, but they were primarily technical and, at least as concerns the no-fly list kids fix, support was clearly bipartisan.

The major (and in some cases, more controversial) sections of the new act are then as follows: Part 1 creates the National Security and Intelligence Review Agency (NSIRA), part 2 creates the IC position, part 3 completely reforms CSE's authority and part 4 amends the CSIS act to tackle some of the criticisms of the disruptive powers regime. It also tackles another ongoing problem confronted by CSIS, related to the collection and storage of metadata and other non-threat related information.[48] Part 7 makes amendments to the Criminal Code's terrorist-advocacy offence, though as with the CSIS disruption regime, it maintains the general thrust of the Bill C-51 initiative and, rather than signalling a policy shift, simply attempts to fix the execution.[49] This paper now turns to a brief overview of these sections noting some – though not all – of the criticisms and issues that may arise.

PART 1 OF BILL C-59: THE CREATION OF NSIRA[50]

Recall that one of the major criticisms of Bill C-51 was that it offered a series of new powers –criminal offences, peace bonds and extensive disruptive powers for CSIS – without confronting the long-recognized problems associated with a lack of review and oversight in the Canadian national security regime. If Canada was going to address its national security landscape, and if it was going to offer extensive new powers, then it was also time to ensure that review and oversight of national security institutions was not siloed. For example, SIRC – the precursor of sorts to NSIRA – was tasked with reviewing CSIS's actions. But SIRC's mandate stopped at the door of CSIS, meaning there was

---

44 See section 2, "Obligation to Issue,": the relevant government departments include: National Defence, Global Affairs Canada, the RCMP, CSIS, the SCE and the CBSA. See Ibid., s. 49.1.

45 Bill C-59.

46 While many departments did indeed already have such information-sharing directives from their ministers, it was historically not always the case and even where such directives existed, these were not always made public.

47 Bill C-59.

48 *X (Re)* [2017] 2 F.C.R. 396, 2016 F.C. 1105.

49 Bill C-59.

50 *National Security and Intelligence Review Agency Act,* s. 8 (s. 2 of Bill C-59).

nobody to perform a whole-of-government review of a CSIS-led response to a national security emergency, nor was there anyone to follow the thread of information shared with other Canadian government agencies (SIRC 2019). Meanwhile, departments like Global Affairs Canada and the Canadian Border Services Agency (CBSA), among others, had no national security review at all.[51]

Following the insights and recommendations of the U.S.'s 9/11 Commission (2004), as well as multiple Canadian commissions of inquiry (Air India 2010, 1: 195-196; Almalki 2008,12; Arar 2006, 364-369), the idea of improved and expanded review was in large part to ensure the legality of the actions of Canada's national security agencies. But though NSIRA's primary task will be ensuring the legality of the actors involved in its investigations, nothing stops it from conducting efficacy reviews as well, particularly should the minister so request.[52]

NSIRA's duty is to review – do after-the-fact analysis of government decisions and operations – rather than to oversee government actions. It does not have the power to say yea or nay in real time to government actions. Specifically, its mandate is to "review any activity carried out by the [CSIS] or the [CSE]",[53] or "any activity carried out by a department that relates to national security or intelligence".[54] It can also take referrals from "a minister of the Crown" related to "national security or intelligence". Finally, it can investigate complaints made to NSIRA with regard to certain agencies[55] and will review significant new ministerial directions issued to CSIS, CSE or other departments where the direction relates to intelligence or national security.[56] NSIRA fills a gap in the security landscape that was filled long ago in places like Britain and the U.S.

Though an expanded national security review is long overdue, during the Bill C-59 debates some controversy arose as to the form of that review. In particular, if NSIRA is to be effective, it will have to be properly staffed and that will take a significant budget. It will also depend on the co-operation of, and good working relationships with, various government departments that will be tasked with providing the information under review. Finally, there will be a cost associated with the increased review functions borne by the departments subject to review – somebody will have to gather information and liaise with NSIRA, which will presumably be easier for an agency like CSIS that was already doing this with SIRC, than Global Affairs which is unaccustomed to review. In that regard, NSIRA should be seen alongside the newly formed National Security and Intelligence

---

51 The Communications Security Establishment (CSE), for example, was reviewed only by its own commissioner. Other bodies, such as the auditor general and information commissioner, also reviewed the CSE, but their mandate was (and is) not related to national security *per se*.

52 Of course, by the time that Bill C-59 was being discussed in earnest, the NSICOP act had created Canada's first (and long overdue) parliamentary oversight body. However, this form of parliamentary review did not extinguish the need for independent, non-political (or at least not by politicians) review of Canadian national security agencies and operations.

53 *National Security and Intelligence Review Act,* s. 8(1)(a).

54 Ibid., s. 8(1)(b).

55 Ibid., s. 8(1)(d).

56 See Ibid., ss. 8(2) and 8(2.1).

Committee of Parliamentarians (NSICOP)[57] (2017) and the IC. While the idea is to bring Canada up to date and in line with its contemporary Five Eyes partners, that makes for three large, important review and/or oversight bodies, exacerbating the cost and bureaucratic concerns (Therrien n.d.).[58]

How certain agencies such as the CBSA or Global Affairs Canada take to review, really for the first time, how they assign and support their staff, and in general how they acculturate to the review process(es) will be worth watching. Likewise, the budget and parliamentary support for NSIRA will most certainly be matters to watch as will the quality (depth, timeliness) of NSIRA's reviews. We will learn much in coming years as to whether its theoretical advantage is able to play out in practice.

PART 2 OF THE BILL: THE CREATION OF THE IC AND SUBSTANTIAL CHANGES TO CSIS DATA COLLECTION AND THE CSE

Bill C-59 also creates another important statutory body – the IC (intelligence commissioner). The IC shall be a "retired judge of a superior court … and hold term for not more than five years".[59] The IC will have responsibility for approving and overseeing (certain) ministerially authorized CSE activities related to electronic data collection, as well as approving the activities of CSIS related to the collection and retention of certain electronic data.[60] Unlike NSIRA, the IC will have the powers of oversight as opposed to review.

Generally, the IC's oversight obligations correspond with the new position's raison d'**ê**tre, which also explains why the IC holds quasi-judicial powers and must be chosen from a pool of retired Federal Court judges. Recall that neither the CSE nor CSIS, particularly as concerns technology, had seen much in the way of legislative amendment for decades. The result was not just that the legal authorities were out of touch with modern national security practice and technological innovations, but that they were significantly out of step with Canadian legal developments. For example, if the RCMP today wishes to place a wiretap on an individual, it will need an authorization from a court, as it would generally need a warrant to search a house. That is because a person's privacy is protected by section 8 of the *Charter,* which protects Canadians from unreasonable search and seizure by the state.

---

57 *National Security and Intelligence Committee of Parliamentarians Act,* S.C. 2017, ch. 15.

58 Indeed, Canada's privacy commissioner, in his testimony on Bill C-59 before the Senate, had the following to say: "Among the recommendations that were not retained, I think the most important one is the one I mentioned in my opening remarks – the difficulty in collaborating with the committee of parliamentarians. Since the committee was struck, I have been invited once to appear before it, and we had an interesting exchange. However, discussions cannot pertain to confidential information I would have learned about through an investigation. They are carried out in a political setting and are rather general. That approach is not without its usefulness, but I cannot give to the committee of parliamentarians more concrete or confidential information I may have learned through investigations. They are also unable to share that kind of information with me, and that is somewhat unfortunate. However, when I look at the bill in its current form, I feel that significant progress has been made overall compared with the current legislation and the bill as it was introduced in the House in the beginning. That is why I recommend that you pass it."

59 *Intelligence Commissioner Act,* s. 4(1).

60 See Ibid., ss. 16-19.

Though the details are rather technical, in general the idea is that a judicially authorized search warrant remains the gold standard whereby a Canadian or person in Canada has a "reasonable expectation of privacy" associated with personal (or personally identifiable) information. But the Supreme Court has asserted that such judicially authorized warrants are not necessarily constitutionally required; instead, a (similar) prior authorization from an impartial actor can suffice where that actor is capable of acting judicially.[61]

So how is this relevant to the current situation? Well, with the new CSE authorities, for example, the agency will have the power to collect all sorts of information for which Canadians might have a "reasonable expectation of privacy". Where such an expectation is present, CSE should have a warrant or something akin to it to justify its searches and seizures. And that is where the IC comes into play. The idea is that, as a retired Federal Court judge, the IC will have both the expertise and the proper understanding of the judicial function to authorize certain search activities by CSE and CSIS that might implicate a "reasonable expectation of privacy" of a Canadian or someone in Canada. Though the regime is novel – Canadians are used to seeing courts perform this function in relation to the police or CSIS – it is so for good reason: the normal court system would not seem to work well for CSE looking to collect, say, publicly available bulk data on Canadians, which implicates a series of processes for which courts do not necessarily have the expertise or time. So, the government had to be innovative and find an alternative that both functioned well in practice – by ensuring that the person overseeing the activities understood the agencies and those activities and was able to act in an informed, efficacious manner – but also functioned in a manner that corresponded to the spirit of the law, which again expects oversight in certain situations by an individual capable of acting judicially. This also explains why the IC has been granted oversight responsibility for some CSE activities that would implicate a reasonable expectation of privacy (collection of foreign intelligence that might scoop up private Canadian data), but not for others, such as CSE's offensive hacking powers, where there are arguably no *Charter* rights implicated and the IC, as a former judge, might have little if any policy expertise. Moreover, CSE has maintained that active cyber-operations presumably be based on foreign intelligence gathering, which would already be covered by both a ministerial authorization and IC oversight.

With the purpose behind the creation of the IC position in mind, let's review the relevant changes to CSIS and discuss the IC's associated functions. We will then move to the introduction of the CSE act, which greatly expands CSE's mandate, as well as the IC's duties as they pertain to the most important new CSE authorities.

CSIS's New Datasets Regime

In recent years, CSIS has run into legal trouble over its acquisition of non-threat-related information (information collected from public sources or in the source of an investigation of a threat, but not pertaining to that threat/person). The Federal Court had criticized both CSIS's retention of non-threat-related metadata (electronic data about data, like geolocation) that it had lawfully collected (as authorized by warrants associated

---

61 *R. v. AM* [2008] S.C.C. 19, 13. Available at https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/4628/index.do. See also *Hunter v. Southam Inc.* [1984] 2 S.C.R. 145, 162. Available at https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/5274/index.co

with threats),[62] and also criticized CSIS for not keeping enough information about investigations for long enough.[63] Partly as a result of these court decisions – primarily the former – and pressing institutional (and public) uncertainty about the scope of CSIS's duties and authorities as concerns datasets[64] – not to mention that CSIS was operating in the 21st century armed with legal authorities created primarily in the 1980s – there was a pressing legal need to resolve the authorities by which CSIS collected, stored and queried certain types of data.[65]

The datasets regime is fairly technical, and its details are beyond the scope of this limited review, though fortunately there are already several excellent and more detailed overviews of the regime available (West 2018a; West and Forcese 2019, 175). Instead, this review will simply address the datasets regime in broad brushstrokes so as to give a sense of what it is attempting to achieve.

The amendments first classify various types of data as being Canadian, publicly available or foreign, with each type treated differently in terms of how CSIS can collect and store the information, and whether (or how) the IC can oversee the data retention and exploitation, etc. The dataset oversight regime then applies only to: (1) the acquisition, retention and exploitation (analysis) of Canadian (as opposed to foreign or publicly available); and (2) bulk data that (3) contain personal information (as defined by the *Privacy Act*) related to (4) non-threat actors (though it may contain other information). The concern of the oversight regime is thus not with threat actors, already covered by warrant regimes and other protections related to CSIS investigations, or to situations where no personal information is collected.

Having thus limited the IC's involvement to a relatively narrow set of circumstances, there are other (non-IC) protections in place related to all sorts of data. For example, before even collecting any dataset, CSIS must satisfy itself that the information collected is relevant to its operations under the CSIS act. It must also ensure that any dataset collection would fall within a pre-approved class authorized by the minister of Public Safety. Finally, Canadian and foreign datasets will be kept separate from CSIS's other holdings (e.g., its data on threats it is investigating). Only designated employees may view and query them in the first instance and they may only pass them along to non-designated employees to use them for domestic intelligence if a query is deemed useful, or if the retention of the dataset is deemed "strictly necessary". Otherwise, the dataset must be destroyed.

One might respond that these are merely internal limitations, but they are meaningful in the context of the legislation as a whole. For example, any classes of data authorized by the minister are subject to the IC's review. If CSIS then wants to retain a Canadian dataset

---

62 See *X (Re)*, [2017] 2 F.C.R. 396, 2016 F.C. 1105.

63 See *Charkaoui v. Canada* [2008] 2 S.C.R. 326, 2008 SCC 38. Available at https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/5482/index.do

64 Datasets are defined in the legislation as "a collection of information stored as an electronic record and characterized by a common subject matter". See cl. 94 amending s. 2 of the CSIS act.

65 See part 4, s. 11.02.

beyond 90 days, it must obtain Federal Court authorization (West and Forcese 2019, 175). However, if it wishes to retain a publicly available dataset indefinitely, it does not need the above authorization, though it must nevertheless delete all irrelevant personal information. NSIRA will continue to monitor CSIS closely and review its activities, just as SIRC did before, a process which can and surely will involve an evaluation of CSIS's acquisition and exploitation of all sorts of data. In fact, each step of the dataset acquisition, retention and use must be recorded and is subject to mandatory periodic auditing, with the reports going to NSIRA. In this way, the regime attempts to scale the oversight and review that it demands in limited situations to ensure that legal requirements for the protection of personal information are properly maintained, while also ensuring that CSIS can do basic data analytics, without undue bureaucratic hurdles, that would be expected of a modern security agency.

By authorizing the acquisition, analysis and retention of such datasets, the new scheme speaks to concerns that Canadian security services need to be in the business, at least, of fairly basic data analytics. However, by placing strict legal restrictions (and oversight by the IC and minister) on each step of the process for non-threat data containing personal information, the scheme attempts to speak to civil libertarian concerns about excessive government surveillance, particularly of non-target groups of individuals. Finally, the new regime speaks to the legal concerns the Federal Court identified regarding CSIS's use of datasets. The scheme attempts to keep everyone happy, or at least make the whole process legally and practically functional.

Of course, that does not mean the regime has succeeded in the eyes of all informed observers. The explicit recognition that data analytics is authorized under the regime certainly does come with a risk of abuse and overreach at minimum. During debate on Bill C-59, the regime was criticized by civil society groups concerned with the breadth of the authority to surveil the Canadian public on such a scale, the scope of the activities overseen by the IC, and whether the regime should allow for such collection activities on Canadians at all (BCCLA 2018; ICLMG 2018). Many, including Privacy Commissioner Daniel Therrien (2018), wanted the publicly available dataset regime to be explicitly overseen by the IC.

In the end, much of the debate will surely centre on how the scheme works in practice, and particularly the quality of oversight. Indeed, the efficacy and propriety of CSIS acquisition, retention and analysis authority may well become one of the issues most worth monitoring in the years to come. Of course, between the creation of NSIRA, the IC and NSICOP, the Canadian public can have added confidence that CSIS's activities are being audited and that the efficacy and propriety of their operations will be brought to Parliament's (NSICOP) attention and the public (through public reports by the bodies). Or, at least, that is the intention of the additional layers of review and oversight that Bill C-59 added to the new permissive powers for security services. In this case, the legislation seems to have done a very good job of meeting the needs of CSIS while ensuring adequate legal protections and oversight. But, as with all things in national security, the devil will be in the details and this new datasets regime bears watching closely.

CSE Finally Gets Stand-Alone Legislation along with an Expanded Mandate … and New Oversight in the Form of the IC

CSE was formed in September 1946 as a communications branch of government, which then became part of DND (CSE n.d.). Prior to the passage of Bill C-59, CSE's entire mandate was found in several pages of part V.1 of the *Department of National Defence Act*. In particular, CSE's mandate was set out in section 273.64 and included only three powers: Mandate A was the "foreign intelligence" authority and allowed CSE to "acquire and use information from the global information infrastructure"; Mandate B was the "cyber defence" mandate that allowed CSE to act in protection of government infrastructure (Global Affairs Canada's infrastructure, for example); and Mandate C was known as the "assistance mandate", which allowed CSE "to provide technical and operational assistance to federal law enforcement and security agencies." The caveat was that if the law enforcement or security agency required a legal warrant to collect information, then they would still need that warrant to get CSE to collect the same.[66]

Bill C-59, via the new CSE act, creates a much more robust legal infrastructure under which CSE will now operate and expands the three mandates to five. Two of them are new (active cyber-operations, sometimes called colloquially and perhaps misleadingly offensive hacking and defensive cyber-operations). Two of them are old (foreign intelligence and assistance mandate), and one (technical and operational assistance) is much expanded.[67] Section 16 of the new CSE act sets out the foreign intelligence mandate to acquire foreign intelligence (eavesdrop) and provide it to the government of Canada.[68] Section 17 provides for a much-expanded cyber-security and information assurance mandate to protect critical electronic and information infrastructure, both public and private.[69] The IC then has oversight responsibility with regard to both sections 16 and 17. Ministerial authorizations of both sections' authorizations are not valid until the IC has provided the minister with written approval. Section 18 provides for a brand new defensive cyber-operations power to protect the section 17 critical infrastructure.[70] Prior to Bill C-59, CSE was limited to protecting federal government networks, but not other networks (private, provincial government and so on); the section 18 defensive cyber-powers thus expand the scope of CSE's protective functions. The minister must provide authorization prior to section 18 powers being enacted and the minister of Foreign Affairs must likewise be "consulted".[71] Section 19 provides for active cyber-operations, which include the authority to "degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security".[72] This new power can

---

66 *National Defence Act*, RSC 1985, ch. N-5, s. 273.1-273.7.

67 See the "Mandate" of the CSE act, s. 15(2) of Bill C-59; for details see also ss. 16-20.

68 CSE act, *supra* note 5 at s. 16.

69 Ibid., s. 17.

70 Ibid., s. 18.

71 Ibid., s. 29(2).

72 Ibid., s. 19.

be authorized by the minister of National Defence and is not subject to IC oversight, which was a matter of some controversy during the debates around C-59 (CIPPIC 2018). However, the minister of Foreign Affairs must have either requested the active cyber-authorizations or consented to them in advance.[73] When conducting either active or defensive cyber-operations, CSE is prohibited from carrying out activities that either "cause, intentionally or by criminal negligence, death or bodily harm to an individual" or "willfully attempt in any manner to obstruct, pervert or defeat the course of justice or democracy".[74] Interestingly, there is no limitation here with respect to property damage, presumably because the intent of some active cyber-operations could be, for example, the destruction of computers or equipment. Finally, section 20 offers the long-held authority for CSE to offer technical and operational assistance to law enforcement and security agencies, the CAF and DND, provided that such agencies come to CSE with appropriate legal instruments authorizing requested actions (e.g., a warrant).[75]

The upshot of this new regime is that CSE is transformed from a primarily passive collector of information, one that intercepts signals for the purposes of advising the government of Canada, to an agency that is also a covert, proactive operator that carries out activities through the global information infrastructure. But, along with these extraordinary new powers comes an expanded legal regime, complete with IC oversight in instances where it is thought a reasonable expectation that the privacy of a Canadian citizen or person in Canada might be implicated, as well as ministerial oversight, and a host of internal requirements and strictures.

For at least two reasons, it will be important to keep a close watch on CSE's new powers and restrictions. First, the powers are far-reaching, and the legal framework in place is novel; how any of it plays out in practice is largely unknown. Second, given the pace of technological change, the new CSE act will certainly need updates and tweaks at more regular intervals than in the past.

Part 4 of Bill C-59: Amending but not Repealing the CSIS Act's Disruptive Powers Regime (SIRC 2016)[76]

Bill C-59 did not remove CSIS's authority to actively disrupt threats; contrary to the McDonald Commission's recommendation, CSIS still retains those new powers. Nor did Bill C-59 remove the powers to act disruptively contrary to other Canadian laws or in

---

73 CSE act*, supra* note 5 at s. 30(2).

74 Ibid.*,* ss. 32(1)(a) and 32(1)(b).

75 Ibid., s. 25.

76 Note also that part 4 of the bill made an important – and very much long overdue – change to the "justification scheme" for CSIS officers and agents, though the amendment appears to have been largely non-controversial. Simply put, SIRC noted in its 2015-2016 annual report that section 25.1 of the Criminal Code does not apply to CSIS agents or officers. Section 25.1 protects designated police officers from criminal liability in the course of their duties where their duties require unlawful conduct. (Think here of an undercover police operative infiltrating – and thus participating in – a terrorist group, which is both a crime and necessary to infiltrate that group). The amendments introduced by Bill C-59 resolve this problem for CSIS agents and officers.

limitation of a *Charter* right.[77] Finally, Bill C-59 did not add any new independent checks to the warrant process: it is still to take place in secret, with one party (the government) present, without an explicit method of appeal or judicial review as exists in the police warrant context.

What Bill C-59 did do was refine the legal architecture surrounding CSIS's new powers, primarily through a host of new limits on their use and scope. This makes the new disruptive regime more likely to be upheld on legal challenge; but it does not guarantee the regime's constitutionality, nor does it address some of the primary legal concerns we saw with the C-51 legal architecture (Nesbitt 2019, 245-265). Let us briefly examine this claim.

Under Bill C-59, the same warrant-authorization process will take place for a *Charter*-limiting activity as existed under C-51. But C-59 puts further limits on the scope of this activity in two ways. First, it expands on Bill C-51's explicit restrictions – those being that CSIS could not conduct disruptive activities that lead to death or bodily harm, the obstruction of justice or a violation of the "sexual integrity of an individual". To this, C-59 added three new sections, which now also prohibit torture or "cruel, inhuman or degrading treatment or punishment", detention and serious property damage where "doing so would endanger the safety of an individual".[78] Second, Bill C-59 further limits CSIS's options by offering a closed list of activities that CSIS might undertake in disruption. The activities (positive) that CSIS can now undertake in limitation of a *Charter* right or other Canadian law include: "altering a communication", including by preventing an email being sent or changing the contents of a website, destroying or otherwise altering equipment (for example, a bomb), fabricating information, conducting or interrupting a financial transaction (e.g., interfering with terrorist financing), impersonating someone or interfering with someone's movement (short of detention).[79]

Together, these new limitations and clarifications play an important legal role. They add clarity to the law by further limiting the scope of activities authorized (important under *Charter* section 1 analyses). These legal additions further "prescribe" the government authorities, which means that a *Charter*-authorizing judge can review proposed CSIS disruptive activities to see if they are of a "type" permitted. What does this mean, precisely, and how is that different from the old regime? Well, the judge is no longer conducting a case-by-case analysis of proposed disruptive activities to save them (individually) under the *Charter* (this was the old C-51 regime), which again is not how the *Charter* works. Rather, under the new C-59 regime the judge is determining if the proposed activities are of a type that has already been specifically authorized under the legislation. In theory then, the judge is not "authorizing" a series of *Charter* violations, but rather reviewing proposed actions to see if they are of a type already authorized by law.

One major problem remains. The disruptive powers explicitly contemplate *Charter* breaches. And *Charter* breaches are not generally authorized under Canadian law, unless they are "saved" under section 1 of the *Charter*. So even if the warrant-authorizing judge

---

77 See CSIS act, s. 12.1(3.2).

78 See Bill C-59, cl. 99.

79 Ibid., cl. 103(1).

is determining whether the legislation specifically authorizes activities, the legislation (and the authorized activities) must first be saved under a *Charter* section 1 analysis for the whole process to be valid. If so saved, then the disruptive activities remain *Charter* breaches, but they are deemed "reasonably justified in a free and democratic society", meaning that they have been properly justified under the *Charter* and received the judicial stamp of approval. So while the Bill C-59 regime has done an end run around the primary Bill C-51 problem – concocting a regime inapposite to the basic functioning of the *Charter* by contemplating a series of *Charter* violations authorized by a judge – it is still a regime that, as a whole, must be authorized after a section 1 save. And this is where the problems lie.

First, the government will presumably have to justify the regime, such that authorizing judges can then implement the judicial section 1 save and authorize prospective warrants. But there seems to be a fatal flaw with the system as originally concocted and then perpetuated under C-59. If the whole process is conducted in secret, without a challenge function, and with no judicial oversight guaranteed past the time of the authorization, then how would the legislation ever be challenged? Even if the legislation were somehow challenged (say, via a public interest challenge, which would take place without any facts of a case or warrant to rely upon), how would anyone challenge specific warrant authorizations and whether they were indeed of an enumerated (and saved) type? And finally, as anyone who follows the police context understands, judicial oversight is important, not just of the proposed warrant, but of the state activity in its execution. Yet in the police context, while this continued judicial oversight is built into legal practice – the defence will often challenge the execution of a warrant, or at least has the opportunity to do so – in the CSIS context, that continued oversight has not been built into the legislation.

Second, even if the above concerns are overcome through practical agreements between CSIS and the courts – for example, warrant-authorizing judges will likely just demand continued oversight of proposed disruptive activities – this does not necessarily mean that the government will win a section 1 *Charter* challenge to the legislation. And here again they face a number of legal obstacles, the most salient being that they will have to justify that the legal regime is "minimally impairing" and not so overbroad so as to capture clearly unintended consequences. That is easier said than done for at least two reasons. First, the Liberal government, like the Conservatives before them, did little to explain why precisely CSIS needed these powers, what it hoped to combat, why CSIS and not the RCMP was the right recipient of the powers, and so on. So we will have to hope that they did, or will do, in practice what they have failed to do publicly, and that is robustly justify the regime by making connections between the specific powers authorized and the specific actions that CSIS might hope to take. Second, these details will greatly matter, because the most obvious question for courts will be why CSIS needs the power to limit any *Charter* right, as opposed to only certain *Charter* rights. Does it need the power to limit the right to be presumed innocent (section 11(d)), the right to be tried within a reasonable time (section 11(b)), or the right to counsel (section 10(b))? Surely, that cannot be the case. But if *Charter* section 10 and 11 rights are all but excluded from the disruptive activities regime – to say nothing of democratic rights like the right to vote under section 3, or equality before the law under section 15 – then

how can a legal regime that purports to include limitations to those rights be minimally impairing and not overly broad? Either the regime intends to capture rights like the presumption of innocence (and thus might be unconstitutional, unless well justified), or it is overly broad (and thus unconstitutional) in that it claims to capture such rights but does not or cannot do so.

At the end of the day, we return to a concern about the C-51 powers, which is not primarily about the granting of those powers at all. Rather, the concern is about the legal architecture constructed to grant those broad powers while ensuring fairness and proper oversight within the legal system. The C-59 regime seems to have eliminated many of the technical problems from the C-51 regime, but not all of them. Some of the most foundational legal concerns remain. In the end, C-59 cannot claim to be much more in practice that C-51 was not, though it did arguably take the legal process more seriously. But in both cases, uncertainty remains – and with it the certainty of costly and time-consuming legal challenges – that results not primarily from complaints with the government authorities, or CSIS activities, but about the process taken to get the legal details right.

One might then respond that if the general disruptive activities can be justified, then perhaps we can do no better on the law, for this is the second attempt to get the legal regime right. Perhaps it is better not to let the perfect be the enemy of the good. But that presumes that no better legal architecture was available and small legislative additions come immediately to mind, which together would go a long way to ensuring the regime's legality and arguably make no difference for what CSIS currently intends to do.

First, a special advocates system could have been built directly into the legislation. Special advocates are now well known to Canada's legal system and have been inserted in the past to legislation that needs an adversarial challenge function, but does not contemplate a defendant or defence lawyer participating. The special advocate then plays the adversarial role of the defence lawyer, though they are also sworn to secrecy, will be security-cleared, would not act on the instruction of a defendant and so on. Special advocates would ensure a proper adversarial process when debating the *Charter* limitations of the disruptive regime, but they would also provide a means to challenge certain decisions and, right from the outset, challenge the legislation, such that it could be saved under section 1 of the *Charter.* At the same time that the special advocates would not be in touch with a proposed CSIS target, their security clearance would ensure there is no concern about the sanctity of proposed CSIS operations. (CSIS warrant authorizations are notoriously slow and legalized processes to begin with and there is little concern that special advocates would impede a rushed process).

As it stands, judges are likely to appoint *amici* (friends of the court), which are court-appointed versions of special advocates (though they are not exactly the same). This is not ideal, for two reasons. First, the duty of the *amici* is to the court, whereas the special advocate has a duty to be oppositional, thus ensuring the sanctity of the adversarial system in these CSIS disruptive warrant hearings. Second, the appointment of *amici* will be tantamount to judicial legislation where Parliament failed to do the obvious. This judicial compensation happens more than one might like, particularly in national security law, but that does not mean we should come to accept it. Moreover, it will invariably lead

to cries of foul regarding the judiciary, when Parliament has put them in a very difficult place: either legislate *amici* where Parliament failed to act (and should have), or overturn the whole disruptive scheme and send the whole thing back to Parliament for revisiting. Neither option is particularly appealing, but the former is certainly less costly and time consuming, and thus we may understand should courts introduce *amici* into these proceedings down the road.

Next, Bill C-59, like C-51, could have inserted a simple requirement that CSIS was obligated to report back to the warrant-authorizing judge on the execution of its disruptive warrants. Again, this is a small thing in practice because, in all likelihood, authorizing judges will demand CSIS keep them apprised of disruptive activities to ensure what takes place is consistent with what was authorized. So perhaps it is pedantic to ask that Parliament, rather than judges, legislate all-but-certain activities. However, that demands the most of Parliament – and asks for really no more than due diligence – while limiting the judicial resort to legislating by another name.

Finally, the Bill C-59 regime should have enumerated the *Charter* sections that CSIS was entitled to limit. A failure to do so risks a finding that the whole regime is unconstitutional, arguably because it authorizes the breach of *Charter* rights (like section 11 due process rights) that in practice neither CSIS nor Parliament intended that they breach. Having failed to do so, the options for judges now would seem to be that the judiciary can (rightly) overturn the legislation as unconstitutional because Parliament failed in its duty to ensure it was minimally impairing and so on, or it can "read in" further limitations to the CSIS disruptive powers (limitations which, again, will likely be non-controversial at least in substance). In an ideal world, we would be demanding (again) that Parliament do its job in legislating, and not then criticizing the judiciary for whatever decision they make between a rock and a hard place, between overturning needed legislation and "reading in" further restrictions when Parliament failed twice to act.

PART 7 OF BILL C-59: AMENDING THE CRIMINAL CODE'S ADVOCATING-TERRORISM OFFENCE

Bill C-59 drafters generally took seriously the criticisms of Bill C-51's advocating-terrorism offence. The updated Bill C-59 offence removed the words "in general" from the reference to "terrorism offences", and, in the words of legal scholars Forcese and Roach (2017), otherwise replaced the "problematic and vague" old provision with "the more familiar and clear criminal law concept of 'counseling another person to commit a terrorism act'." The new offence now reads:

> **83.221** (1) Every person who counsels another person to commit a terrorism offence without identifying a specific terrorism offence is guilty of an indictable offence and is liable to imprisonment for a term of not more than five years.[80]

[80] Criminal Code, s. 83.221. Subsection 2 clarifies that the offence may be committed even if the person counselled to commit a terrorist offence does not actually do so.

Though the change in language is certainly admirable, in many ways it reinforces the most salient concern with the C-51 language: if this is nothing more than a counselling offence, then given that section 22 of the Criminal Code proscribes counselling any offence,[81] what precisely does this new counselling-terrorism offence add? There seem to be two responses to this question. First, the new offence is redundant, which at best makes the offence unnecessary, confusing and difficult to grasp for non-lawyers trying to understand the Criminal Code*,* and at worst will lead to confusion and expensive litigation. Second, the offence is not redundant, in which case its meaning is again unclear as it was under C-51, which in turn makes it difficult and expensive to charge and prosecute. The best-case scenario is somewhere between mildly and unnecessarily expensive, slightly confusing and otherwise harmless, and the worst-case scenario is worse than that.

The result of the C-59 update is clearer language, but otherwise the existence of this advocacy or counselling offence further ensconces much confusion and thus leaves much to be desired. C-59 seems to have technically amended the terrorist-advocacy offence without either repealing it or clarifying how the offence itself provides much new to the Criminal Code*.*

Moreover, other legal concerns regarding the C-51 offence are held over in C-59. Most notably, other speech offences like hate speech and genocide have caveats built into them. For example, the "willful promotion of hatred" offence offers defences for truth, religious opinion and public interest.[82] These exceptions to the scope of the speech offences were constitutionally mandated.[83] So, given that the new terrorism-advocacy offence does not include the same carve-outs, will it be rife for constitutional challenge? On the one hand, one would think so as this seems like a fairly basic baseline for other speech offences, so why would this offence be any different? On the other hand, one can see a clear difference here: the advocacy offence was trying to get at precisely the type of speech (Islamist extremist glorification) which is both truly held by that extremely small segment of the population that abides by that ideology and likewise, on the understanding of these extremists, is religiously held. Of course, one can respond that this is no valid religious belief, but this asks the courts to wade into legitimate versus illegitimate religious beliefs, a task about which both courts and society have rightly been wary. Where this leaves the advocacy – now counselling – terrorism offence is anyone's guess.

One other question remains unanswered, succinctly asked again by Forcese and Roach (2016): "how the new speech crime will dovetail (or not) with the government's promised new program to counter violent extremism. An essential ingredient of any such program is speaking to those with extremist views, if only to dissuade. But if voicing views in the

---

81 Ibid*.,* s. 22.

82 Ibid., s. 319(3).

83 As noted earlier, the Supreme Court considered the constitutionality of the "wilful promotion of hatred" offence in *R. v. Keegstra*. The Court said the defences "are hence intended to aid in making the scope of the wilful promotion of hatred more explicit … The result is that what danger exists that s. 319(2) is overbroad or unduly vague, or will be perceived as such, is significantly reduced." This indicates that, absent the defences, the Court would have been much more willing to strike down the provision as unconstitutional.

wrong place is a crime, those practicing counter-extremism must worry that their efforts will become a stalking horse for a police investigation." Canada's CVE (countering violent extremism) work remains in its infancy. But the general concern that proscribing speech will capture both the bad and the good (that which is needed for democratic debate, or in this case to allow people to talk openly so as to counter certain messages) is always a fine line. Much might depend not just on the new offence, but how and when it is used in practice. It is something that criminal and national security law scholars will surely follow in the years to come.

CONCLUSION: NEXT STEPS AND WHAT'S LEFT TO DO?

In general, Bill C-59 is substantially broader in scope than Bill C-51 and provides a more robust legal architecture to support the new powers that it confers on Canada's security agencies. The powers it authorizes are thus more likely to withstand judicial scrutiny and more likely to be usable by national security agencies. Moreover, Bill C-59 responds to long-standing concerns about the lack of systemic review and oversight in the Canadian system. The bill should bring with it greater accountability and transparency due to propriety reviews. It should also arguably bring greater efficacy as we all get a better sense of the Canadian national security landscape, what processes exist or are absent, and how agencies communicate with one another. This is undoubtedly a good-news story resulting from the C-51 and C-59 processes.

But we must hope that tactical and technological developments do not overtake the legal mandates associated with Canadian national security agencies. With the pace of society today, Canada cannot again wait 30 years for sweeping legislative reforms. Rather, such reform must be introduced in a more incremental and consistent manner. Again, NSIRA (and the IC and NSICOP) have a role to play here – they may bring problems, legal and otherwise, as well as outdated or non-existent authorities to Parliament's attention. But at the end of the day, Parliament must place a real priority on national security, one that requires thoughtful, proactive policy commitments and continued vigilance. Whether this takes place in the years to come remains to be seen, though that does not diminish the need for Canadians of all stripes to push for continued vigilance.

In the meantime, there is a host of pressing national security issues with which the next government might engage in the short term. First is the need to address Canada's "intelligence-to-evidence" conundrum (Forcese 2019; West 2018b, 57);[84] that is, how raw intelligence collected in the field for non-legal purposes is turned (or not turned, as is often the case in Canada) into usable evidence which Canadian courts can use during prosecutions. Right now, I understand there is a push within government and without to find a way forward that improves on Canada's current system, which is plagued by disclosure problems before the courts, delayed trials, ongoing issues with the use of

84 Two excellent recent legal articles discuss this conundrum, and potential solutions. See Leah West, "The Problem of 'Relevance': Intelligence to Evidence Lessons from UK Terrorism Prosecutions," 41 *Manitoba Law Journal* 4 (2018), 57. See also Craig Forcese, "Threading the Needle: Structural Reform & Canada's Intelligence-to-Evidence Dilemma," 42 *Manitoba Law Journal* 4 (2019), 131.

foreign intelligence in Canadian courts and so on. If the solution were simple, we would have implemented it. So there is work to do. But right now, there is arguably no more pressing issue in Canadian national security than tackling this conundrum.[85]

At the same time, and perhaps in part due to the investigative and disclosure issues that plague our system, Canada has a poor record of prosecuting money laundering, terrorist financing, and most recently, far-right extremism. We have not even attempted to use our Criminal Code offences to prosecute someone who has returned from the battlefield in Syria – an interesting development, considering we have Criminal Code offences designed to tackle this very problem[86] of Canadians who go abroad to become foreign fighters and then return to Canada. Governments will almost surely have to provide greater resources and political attention to these issues, which will demand some hard choices. But if Canada is to improve its prosecution record and tackle these important national security and social issues, then such parliamentary leadership is necessary. To start, a more comprehensive look at each of these issues, where the problems lie, and what solutions might be available would be an excellent task for a parliamentary committee such as the Standing Committee on Public Safety and National Security or the Senate Committee on National Security and Defence.

---

85 There is good news already that this issue is front of mind with bureaucrats and parliamentarians. The Department of Justice has undertaken a limited public consultation on intelligence to evidence and the dual court system. Moreover, and significantly, led by Senator Marc Gold, the Senate is seized by the intelligence-to-evidence issue. See Canada. Parliament, *Debates of the Senate*, Motion by the Honourable Marc Gold, *Motion to Authorize Committee to Study the Body of Issues Known as "Intelligence to Evidence,"* (Dec. 11, 2019).

86 See Criminal Code, ss. 83.181 and 83.191 ("Leaving Canada to Participate in Activity of Terrorist Group" and "Leaving Canada to Facilitate Terrorist Activity" respectively).

REFERENCES

Block, Elizabeth, James L. Turk, Sharon Polsky, Sid Shniad, et al. 2018. "Civil Society Statement Regarding Bill C-59, An Act Respecting National Security Matters." International Civil Liberties Monitoring Group. April 5. Available at www.iclmg.ca/civil-society-statement-c59/ Accessed July 2019.

British Columbia Civil Liberties Association (BCCLA). 2018. "Written Submissions of the British Columbia Civil Liberties Association to the Standing Committee on Public Safety and National Security Regarding Bill C-59, An Act Respecting National Security Matters." Jan. 30. Available at http://www.bccla.org/wpcontent/uploads/2018/02/2017-01-30Written-Submissions-of-the-BCCLA-to-SECU_Bill-C-59.pdf Accessed July 2019.

Communications Security Establishment (CSE). n.d. "History." Available at www.cse-cst.gc.ca/en/history-histoire Accessed September 2019.

Conservative Party of Canada. 2015. *Protect Our Economy*. Available at www.conservative.ca/media/plan/conservative-platform-en.pdf Accessed July 2019.

Coudhury, Fufyal, and Helen Fenwick. 2011. "The Impact of Counter-Terrorism Measures on Muslim Communities." Research report no. 72. U.K., Equality and Human Rights Commission. Manchester: Equality and Human Rights Commission.

Elghawaby, Amira. 2016. "Children Banned from Flying? Sadly, It's not that Uncommon." *Globe and Mail.* Jan. 8. Available at www.theglobeandmail.com/opinion/children-banned-from-flying-sadly-its-not-that-uncommon/article28059610/ Accessed July 2019.

Forcese, Craig. 2019. "Threading the Needle: Structural Reform & Canada's Intelligence-to-Evidence Dilemma." 42 *Manitoba Law Journal* 4.

Forcese, Craig, and Kent Roach. 2015a. "Bill C-51 Backgrounder #3: Sharing Information and Lost Lessons from the Maher Arar Experience." Feb. 16. Available at http://www.ssrn.com/abstract=2565886

———. 2015b. *False Security: The Radicalization of Canadian Anti-Terrorism.* Toronto: Irwin Law.

———. 2016. "Renewed Bill C-51 Questions: Balancing National Security with Civil Liberty." *Globe and Mail.* Oct. 17. Available at www.theglobeandmail.com/opinion/renewed-bill-c-51-questions-balancing-national-security-with-civil-liberty/article32393193/ Accessed July 2019.

———. 2017. "A Report Card on the National Security Bill." *Policy Options.* Available at www.law.utoronto.ca/news/prof-kent-roach-co-authors-report-card-national-security-bill Accessed July 2019.

Gadzo, Mersiha. 2016. "You Should be Worried about Canada's Anti-Terrorism Act." CBC News. Nov. 13. Available at www.cbc.ca/news/canada/manitoba/canada-anti-terrorism-bill-c-51-opinion-1.3845559 Accessed July 2019.

International Civil Liberties Monitoring Group (ICLMG). n.d. "Peace Bonds and Preventative Detention." Available at www.iclmg.ca/issues/peace-bonds/ Accessed July 2019.

Liberal Party of Canada. 2015. *A New Plan for a Strong Middle Class*. Available at www.liberal.ca/wp-content/uploads/2015/10/New-plan-for-a-strong-middle-class.pdf Accessed July 2019.

Macleod, Ian. 2015. "Anti-Terror Bill: Experts Worry about Sweeping Powers for CSIS." *Ottawa Citizen.* Feb. 7. Available at www.ottawacitizen.com/news/politics/anti-terror-bill-experts-worry-about-sweeping-powers-for-csis Accessed July 2019.

National Commission on Terrorist Attacks Upon the United States. 2004. *The 9/11 Commission Report*. New York: Norton.

Nesbitt, Michael. 2015. "CSIS's New Disruptive Powers, Grey Holes, and the Rule of Law." *Canadian Yearbook of Human Rights*, no. 1.1. Available at www.hri.ca/wp-content/uploads/2017/10/ottawau_canadianyearbookofhumanrights_vol1_2015.pdf Accessed September 2019.

———. 2019. "Bill C-59 and CSIS's 'New' Powers to Disrupt Terrorist Threats: Holding the *Charter*-Limiting Regime to (Constitutional) Account." 57 *Alberta Law Review* 1.

New Democratic Party of Canada. 2015. "Building the Country of our Dreams." Available at www.s3.documentcloud.org/documents/2454378/2015-ndp-platform-en.pdf Accessed July 2019.

#NoFlyListKids. n.d. "100,000 Affected Canadians." Available at www.noflylistkids.ca/en/100000-canadians/ Accessed July 15, 2019.

Office of the Privacy Commissioner of Canada. 2017. *Review of the Operationalization of the Security of Canada Information Sharing Act.* Available at www.priv.gc.ca/en/opc-actions-and-decisions/audits/ar-vr_scisa_2017/ Accessed July 2019.

Public Safety and Emergency Preparedness (PSEP). 2016. "Our Security, Our Rights: National Security Green Paper, 2016." Government of Canada. Available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016/ntnl-scrt-grn-ppr-2016-en.pdf Accessed July 2019.

Public Works (Air India). 2010. Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182. *Air India Flight 182: A Canadian Tragedy – The Overview,* vol. 1. Government of Canada.

Public Works and Government Services Canada (Arar). 2006. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations*. Government of Canada.

———. (Almaki). 2008. Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin. *Supplement to Public Report*.

Sallot, Jeffrey. 2006. "Royal Commission on Inquiry into Certain Activities of the Royal Canadian Mounted Police." *The Canadian Encyclopedia*. Available at https://www.thecanadianencyclopedia.ca/en/article/royal-commission-on-inquiry-into-certain-activities-of-the-royal-canadian-mounted-police Accessed July 2019.

Samuelson-Glushko Canadian Internet Policy and Public Interest Clinic and the Citizen Lab. 2018. "Government's Defence of Proposed CSE Act Falls Short." Available at https://cippic.ca/news/C59_CSE_justifications_fall_short Accessed July 2019.

Security Intelligence Review Committee (SIRC). 2016. *Annual Report 2015-2016: Maintaining Momentum*. Government of Canada.

———. 2019. "All Government of Canada National Security and Intelligence Activities now Subject to Independent Expert Review." Government of Canada. News release. July 17. Available at https://www.newswire.ca/news-releases/all-government-of-canada-national-security-and-intelligence-activities-now-subject-to-independent-expert-review-858523391.html Accessed July 2019.

Therrien, Daniel. Privacy Commissioner of Canada. 2018. "Submission to the Standing Committee on Public Safety and National Security Regarding the Review of Bill C-59, An Act Respecting National Security Matters." March 5. Available at https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2018/parl_sub_180305/?t=1&cn=ZmxleGlibGVfcmVjc18y&refsrc=email&iid=82a21feadfa2441ebf516ad9d47cd7af&uid=527852203&nid=244+272699400 Accessed July 2019.

———. Privacy Commissioner of Canada. 2019. April 29. Available at https://sencanada.ca/en/Content/SEN/Committee/421/secd/54717-e Accessed July 2019.

Tucker, Erica. 2014. "Soldier Killed in what Harper Calls 'Terrorist' Attack in Ottawa." Global News. Oct. 22. Available at www.globalnews.ca/news/1628313/shots-fired-at-war-memorial-in-ottawa-says-witness/

Tucker, Erica, and Adam Frisk. 2014. "Canadian Soldier Dies in Quebec Attack 'Linked to Terrorist Ideology'." Global News. Oct. 21. Available at www.globalnews.ca/news/1625585/canadian-soldier-struck-by-car-in-quebec-has-died/

West, Leah. 2018a. "Canada Tries Domestic Bulk Collection: It Just Might Work." Lawfare Blog. March 26. Available at https://www.lawfareblog.com/canada-tries-domestic-bulk-collection-it-just-might-work Accessed October 2019.

———. 2018b. "The Problem of 'Relevance': Intelligence to Evidence Lessons from UK Terrorism Prosecutions." 41 *Manitoba Law Journal* 4.

West, Leah, and Craig Forcese. 2019. "Building Haystacks: Information Retention and Data Exploitation by the Canadian Security Intelligence Service." 57 *Alberta Law Review* 1.

Zilio, Michelle, and Janice Dickson. 2019. "Parents of Kids Wrongly Flagged by No-Fly List Urge Senate to Pass Legislative Changes Quickly." *Globe and Mail*. May 6. Available at www.theglobeandmail.com/politics/article-parents-of-kids-wrongly-flagged-by-no-fly-list-urge-senate-to-pass/

About the Author

Dr. Michael Nesbitt is an Assistant Professor with the University of Calgary, Faculty of Law, a senior fellow at the University of Calgary's *Centre for Military, Security and Strategic Studies*, a Fellow with the *Canadian Global Affairs Institute*, and a Senior Research Affiliate with the *Canadian Network for Research on Terrorism, Security and Society*. Dr. Nesbitt teaches and researches in the areas of national security law and policy, anti-terrorism law, criminal law, as well as the legal and policy issues surrounding economic sanctions. Before joining the Faculty of Law, Dr. Nesbitt practiced law and worked in the areas of Middle East policy, human rights, international sanctions and terrorism for Global Affairs Canada. He has also worked for Canada's Department of Justice and internationally for the United Nations' International Criminal Tribunal for the Former Yugoslavia in the Appeals Chamber.

ABOUT THE SCHOOL OF PUBLIC POLICY

The School of Public Policy has become the flagship school of its kind in Canada by providing a practical, global and focused perspective on public policy analysis and practice in areas of energy and environmental policy, international policy and economic and social policy that is unique in Canada.

The mission of The School of Public Policy is to strengthen Canada's public service, institutions and economic performance for the betterment of our families, communities and country. We do this by:

- *Building capacity in Government* through the formal training of public servants in degree and non-degree programs, giving the people charged with making public policy work for Canada the hands-on expertise to represent our vital interests both here and abroad;
- *Improving Public Policy Discourse outside Government* through executive and strategic assessment programs, building a stronger understanding of what makes public policy work for those outside of the public sector and helps everyday Canadians make informed decisions on the politics that will shape their futures;
- *Providing a Global Perspective on Public Policy Research* through international collaborations, education, and community outreach programs, bringing global best practices to bear on Canadian public policy, resulting in decisions that benefit all people for the long term, not a few people for the short term.

The School of Public Policy relies on industry experts and practitioners, as well as academics, to conduct research in their areas of expertise. Using experts and practitioners is what makes our research especially relevant and applicable. Authors may produce research in an area which they have a personal or professional stake. That is why The School subjects all Research Papers to a double anonymous peer review. Then, once reviewers comments have been reflected, the work is reviewed again by one of our Scientific Directors to ensure the accuracy and validity of analysis and data.

The School of Public Policy
University of Calgary, Downtown Campus
906 8th Avenue S.W., 5th Floor
Calgary, Alberta T2P 1H9
Phone: 403 210 3802

DISTRIBUTION
Our publications are available online at www.policyschool.ca.

DISCLAIMER
The opinions expressed in these publications are the authors' alone and therefore do not necessarily reflect the opinions of the supporters, staff, or boards of The School of Public Policy.

ISSN
ISSN 2560-8312 The School of Public Policy Publications (Print)
ISSN 2560-8320 The School of Public Policy Publications (Online)

DATE OF ISSUE
May 2020

MEDIA INQUIRIES AND INFORMATION
For media inquiries, please contact Morten Paulsen at 403-220-2540. Our web site, www.policyschool.ca, contains more information about The School's events, publications, and staff.

DEVELOPMENT
For information about contributing to The School of Public Policy, please contact Catherine Scheers by telephone at 403-210-6213 or by e-mail at catherine.scheers@ucalgary.ca.

RECENT PUBLICATIONS BY THE SCHOOL OF PUBLIC POLICY

CONSIDERATIONS FOR BASIC INCOME AS A COVID-19 RESPONSE
https://www.policyschool.ca/wp-content/uploads/2020/05/Basic-Income-Green-Kesselman-Tedds.pdf
David Green, Jonathan Rhys Kesselman and Lindsay Tedds | May 2020

ECONOMIC POLICY TRENDS: THE BANK OF CANADA'S RESPONSE TO COVID-19 AND THE COLLAPSE IN WORLD OIL PRICES
https://www.policyschool.ca/wp-content/uploads/2020/05/Econ-Policy-Trends-BOC-COVID-Oil-Prices.pdf
Scott Cameron | May 2020

ECONOMIC POLICY TRENDS: UNEQUAL BURDEN: LEARNING FROM CANADA'S RESPONSES TO THE INFLUENZA PANDEMIC OF 1918-20
https://www.policyschool.ca/wp-content/uploads/2020/05/Econ-Policy-Trends-Influenza.pdf
Shawn W. Brackett | May 2020

ALBERTA'S CIVIL SOCIETY PRE-AND-POST-COVID-19: WHAT'S GOVERNMENT GOT TO DO WITH IT?
https://www.policyschool.ca/wp-content/uploads/2020/05/Civil-Society-Turner-Escamilla.pdf
Alina Turner and Camilo Camacho Escamilla | May 2020

RUSSIAN GEOPOLITICAL OBJECTIVES IN THE CURRENT OIL PRICE CRISIS AND THE IMPLICATIONS FOR CANADA
https://www.policyschool.ca/wp-content/uploads/2020/05/Russian-Geopolitical-Sukhankin.pdf
Sergey Sukhankin | May 2020

SOCIAL POLICY TRENDS: ECONOMIC AND EMOTIONAL DISTRESS
https://www.policyschool.ca/wp-content/uploads/2020/05/Social-Policy-Trends-Stress.pdf
Ron Kneebone | May 2020

NO GOING BACK: THE IMPACT OF ILO CONVENTION 169 ON LATIN AMERICA IN COMPARATIVE PERSPECTIVE
https://www.policyschool.ca/wp-content/uploads/2020/04/final_No-Going-Back-Aylwin-Policzer.pdf
José Aylwin and Pablo Policzer | April 2020

ECONOMIC POLICY TRENDS: THE DOMESTIC VIOLENCE CRISIS AND COVID-19: CAN SHORT-TERM RENTALS HELP?
https://www.policyschool.ca/wp-content/uploads/2020/04/Economic-Policy-Trends-Domestic-Violence.pdf
Daria Crisan | April 2020

YOU SAY USMCA OR T-MEC AND I SAY CUSMA: THE NEW NAFTA – LET'S CALL THE WHOLE THING ON
https://www.policyschool.ca/wp-content/uploads/2020/04/final2_NAFTA-Trade-Beaulieu-Klemen.pdf
Eugene Beaulieu and Dylan Klemen | April 2020

ECONOMIC POLICY TRENDS: COVID-19 AND RECENT POST-SECONDARY GRADUATES
https://www.policyschool.ca/wp-content/uploads/2020/04/econ-policy-trends-post-secondary-covid.pdf
Christine Neill and Kelly Foley | April 2020

ECONOMIC POLICY TRENDS: POST-SECONDARY FINANCIAL AID AND THE PANDEMIC
https://www.policyschool.ca/wp-content/uploads/2020/04/econ-trends-Post-Secondary-Financial-Aid.pdf
Christine Neill and Kelly Foley | April 2020

ENERGY AND ENVIRONMENTAL POLICY TRENDS: POWER DEMAND IN THE TIME OF COVID-19
https://www.policyschool.ca/wp-content/uploads/2020/04/EE-policy-trends-power-and-covid.pdf
Blake Shaffer, Andrew Leach and Nic Rivers | April 2020

HEALTH INNOVATION AND COMMERCIALIZATION ECOSYSTEMS AND PUBLIC HEALTH EMERGENCY RESPONSE SYSTEMS
https://www.policyschool.ca/wp-content/uploads/2020/04/Precision-Health-Scott-Zwicker.pdf
Craig Scott and Jennifer D. Zwicker | April 2020