FORUM INTRODUCTION

BILL C-59, *AN ACT RESPECTING NATIONAL SECURITY MATTERS*: WHAT IT DOES AND WHY IT MATTERS

MICHAEL NESBITT* AND LEAH WEST**

On 21 June 2019, Parliament initiated a historic transformation of Canada's national security landscape, when it passed into law Bill C-59, *An Act respecting national security matters*.[1] It is no exaggeration to say that this is the most wide-reaching and important update to Canada's national security legal framework and organizational structure since at least 1984, when the *Canadian Security Intelligence Service Act* hived off the security and intelligence functions of the Royal Canadian Mounted Police (RCMP) to create the Canadian Security and Intelligence Service (CSIS).[2] Among other things, the *ATA* 2017 created an entirely new oversight body in the form of the Intelligence Commissioner (IC), radically redesigned intelligence review, reformed and added new lines of operations for the Communications Security Establishment (CSE) including brand-new offensive and defensive cyber authorities, and made substantial changes to the breadth and scope of the information CSIS can collect. These changes will assuredly be both vital to the protection of Canadian national security and controversial with regards to the civil liberties of Canadians in the years to come.

Consequently, anyone interested in Canadian national security law and policy, both in terms of how it keeps us safe and how it protects or threatens our rights and freedoms, must understand the implications and uncertainties arising from the *ATA* 2017. We hope that this Forum in the *Alberta Law Review* offers a starting place for just such an understanding, providing not only an introduction to some of the more complicated issues but a place where other researchers and practitioners can begin, what we hope will become, a thoughtful and ongoing evaluation of the *Act*. We think that the topics addressed by the contributing authors in this Forum speak to some of the fundamental issues that will arise in the days and years ahead.

This Forum also aims to inspire others to engage academically with questions arising from Canadian national security law and policy. Increased critical and sympathetic engagement with this area of the law from a Canadian and comparative perspective is needed, and vitally important now more than ever. This Forum is intended to be a launching point for future research and an example of approaches to the analysis of national security law that might be extended outwards to other aspects of the *ATA* 2017 and beyond. Thus, the articles herein do not canvas all of the legal issues, potential solutions, or unanswered questions raised by the legislation; nor could they. Rather, they were selected to spark new ideas, inspire debate, and,

* Assistant Professor of Law, University of Calgary, Faculty of Law; Senior Fellow with the Centre for Military, Security and Strategic Studies; and Fellow with the Canadian Global Affairs Institute.

** Lecturer of National Security and Intelligence at the Norman Paterson School of International Affairs, Carleton University.

1 Bill C-59, *An Act respecting national security matters*, 1st Sess, 42nd Parl, 2019 (assented to 21 June 2019), SC 2019, c 13 [*ATA* 2017].

2 *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 [*CSIS Act*].

we hope, lead to a larger, more robust conversation not just about current national security practices, but about what the future holds.

With this purpose in mind, the remainder of this introductory chapter will offer a very brief overview of the *ATA* 2017. This review is coupled with summaries of the four articles prepared for this Forum as they pertain to the relevant *ATA* 2017 amendments. We end by drawing together some of the overarching themes and lessons from these four articles.

AN ACT RESPECTING NATIONAL SECURITY MATTERS: WHAT IT DID AND WHY IT MATTERS

The *ATA* 2017 runs over 150 pages, all of which pertains to national security matters. It is structured in ten Parts, which offer reforms that touch on every Canadian government department that collects, disseminates, and receives information in the national security space, including departments not often thought of for their role in national security, such as Global Affairs Canada. The *ATA* 2017 also creates two brand new and vitally important bodies: the National Security and Intelligence Review Agency (NSIRA)[3] and the IC,[4] and it is with the creation of these bodies that the *Act* begins.

Part 1 of the *ATA* 2017 creates the NSIRA, tasked with reviewing the actions and decision-making of national security actors, and information sharing and cooperation within and across government agencies as it pertains to national security matters. This review function serves as an after-the-fact audit of the lawfulness and compliance of these national security agencies.

Before NSIRA there was no one body tasked to review whole-of-government national security information sharing and operations; review of CSIS, CSE, and (to a lesser extent) the RCMP was the responsibility of three separate and siloed bodies.[5] In other words, there was no single entity with the mandate to follow the thread of intelligence operations or information sharing from department to department. Canada's review bodies were "constrained from following the information of the agency they examine into other Government of Canada institutions and from performing joint reviews."[6] These constraints, made it "increasingly difficult for [the Security Intelligence Review Committee] to provide robust assurances on CSIS's activities to Parliament and Canadians."[7] This was a warning issued for years by numerous parliamentary committees, as well as the Arar and Air India commissions of inquiry.[8]

---

3 *National Security and Intelligence Review Agency Act*, s 8, being Part 1 of the *ATA* 2017, *supra* note 1 [*NSIRA Act*].

4 *Intelligence Commissioner Act*, s 12, being Part 2 of the *ATA* 2017, *ibid* [*IC Act*].

5 Of course, actors like the Auditor General and Information Commissioner have been able to review the activities of departments across government, but their mandates are not focused on national security operations and information sharing and they do not generally have the expertise to review the efficacy of inter-department national security cooperation, for example.

6 See Senate, Standing Senate Committee on National Security and Defence, *Evidence*, 41-2, No 16 (23 April 2015) (Michael Doucet).

7 *Ibid*.

8 House of Commons, *Review of the Findings and Recommendations Arising from the Iacobucci and O'Connor Inquiries: Report of the Standing Committee on Public Safety and National Security* (June 2009) (Chair: Garry Breitkreuz), Recommendation 5; House of Commons, *Rights, Limits, Security: A Comprehensive Review of the Anti-Terrorism Act and Related Issues: Final Report of the Standing Committee on Public Safety and National Security* (March 2007) (Chair: Garry Breitkreuz),

Moreover, the fact that many other important government departments had no national security review at all, including Global Affairs Canada, the Canada Border Service Agency (CBSA), the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), and others, compounded the problem. In the result, Canada was completely out of step with its closest intelligence sharing partners, the United States, the United Kingdom, Australia, and New Zealand, which together make up the so-called "Five Eyes Alliance." The creation of the NSIRA thus fills a longstanding and significant accountability gap in the Canadian national security and intelligence community.

Part 1.1 of the *ATA* 2017, a late addition to the Bill, enacts the *Avoiding Complicity in Mistreatment of Foreign Entities Act*.[9] This *Act* is a partial response to the case of Maher Arar, where a subsequent commission of inquiry into his treatment found multiple problems with the way Canadian intelligence agencies shared information abroad.[10] As such, Part 1.1 creates a binding obligation on National Defence, Global Affairs Canada, the RCMP, CSIS, the CSE, and CBSA to issue public Ministerial directions on how these departments govern foreign information sharing. Generally, this includes both information Canadian agencies send abroad, as well as how information is collected from foreign partners and used in Canadian operations — where there is a risk that the information is derived from or may contribute to mistreatment.

Part 2 creates the office of the IC, which serves an important oversight role for both CSE and CSIS. The IC and his secretariat is Canada's first national security oversight body responsible for assessing and approving the reasonableness of an elected official's decision before a security agency can act on that decision. This process of oversight is a critical element in terms of the constitutionality of CSE's and CSIS's electronic information collection regimes modified by the *ATA* 2017, which may result in the acquisition of personal information about Canadians and persons within Canada. Personally identifiable information may attract a reasonable expectation of privacy, triggering protections under section 8 of the *Canadian Charter of Rights and Freedoms*, which protects everyone against unreasonable search and seizure.[11] While a search warrant issued by a judge is the gold standard when it comes to protecting section 8 rights and ensuring searches by the state are "reasonable," they are not constitutionally required if a state agent instead obtains prior authorization from a neutral and impartial actor capable of acting judicially.[12]

Under the *ATA* 2017, CSE and CSIS may leverage certain collection authorities with the approval of an elected official or their designate (most notably the collection of foreign datasets by CSIS and foreign signals intelligence by CSE). The Minister of Public Safety and the Minister of National Defence are not neutral or impartial actors capable of acting

---

Recommendations 58–60; Senate, *Security, Freedom, and the Complex Terrorist Threat: Positive Steps Ahead: Interim Report of the Special Senate Committee on Anti-Terrorism* (March 2011) (Chair: Hon Hugh Segal), Recommendation 16; Canada, Privy Council, *Report of the Events Relating to Maher Arar*, by Dennis R O'Connor (Ottawa: Privy Council, 2006) at, for example, 591–95 [Arar COI]; US, 9/11 Commission, *The 9/11 Commission Report* (Washington, DC: 9/11 Commission, 2004) at 411 [*9/11 Commission Report*].

9 Being Part 1.1 of the *ATA* 2017, *supra* note 1.

10 See generally Arar COI, *ibid*.

11 See Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*].

12 *R v AM*, 2008 SCC 19 at para 13; *Hunter v Southam Inc*, [1984] 2 SCR 145 at 162.

judicially.[13] Thus, the IC's review of Ministerial decision-making is intended to ensure CSIS and CSE activities are constitutionally compliant in a more expedient and deferential manner than bringing applications before a Federal Court judge. The IC also plays a role in CSIS's new justification regime which permits regulated violations of the law by CSIS employees and individuals assisting them during intelligence investigations. Based on the recommendation of the Prime Minister, the first IC, the Honourable Jean-Pierre Plouffe, was appointed by the Governor in Council in the summer of 2019.[14]

Part 3 of the *ATA* 2017 greatly reforms the CSE and expands its "mandates." CSE's history dates back to the Second World War, but it was given its first statutory mandate in 2001 when Parliament amended the *National Defence Act* (*NDA*)[15] in the wake of 9/11. Under the *NDA*, CSE's tripartite mandate included: foreign electronic intelligence, cybersecurity, and assistance to federal law enforcement and security agencies. The passage of the *ATA* 2017 not only created a more detailed legal architecture for CSE, but it also expanded the CSE's lines of operations from three to five, and revamped its cybersecurity and information assurance mandate by empowering CSE to work directly with the private sector and other levels of government.

CSE's two new mandates include active and defensive cyber operations. These broad powers authorize CSE to actively engage and respond to foreign actors who threaten Canadian security interests. First, CSE's defensive cyber mandate authorizes it "to carry out activities on or through the global information infrastructure to help protect (a) federal institutions' electronic information and information infrastructures; and (b) electronic information and information infrastructures," designated as being of importance to the Government of Canada.[16] Before the *ATA* 2017, CSE could assist the Government of Canada in its effort to protect cyber networks as part of its cybersecurity mandate, but it did not have the authority to take action outside government networks to defend or deter cyber-attacks against Canada.

CSE's "active cyber" mandate is even broader. It authorizes the CSE to "carry out activities on or through the global information infrastructure 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."[17] A matter of some controversy, use of these new powers is authorized by the Minister of National Defence and not subject to oversight by the IC.

---

13 For further discussion on this point, see Tamir Israel, "Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation," in Michael Geist, ed, *Law, Privacy and Surveillance in Canada in the Post-Snowden Era* (Ottawa: Univeristy of Ottawa Press, 2015) 71 at 77.

14 *IC Act*, *supra* note 4, s 4(1).

15 RSC 1985, c N-5.

16 *Communications Security Establishment Act*, s 18, being Part 3 of the *ATA* 2017, *supra* note 1 [*CSE Act*].

17 *IC Act*, *supra* note 4, s 19. Section 2 of the *CSE Act* explains that: the "global information infrastructure includes electromagnetic emissions, any equipment producing such emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those emissions, that equipment, those systems or those networks": *CSE Act*, *ibid*.

Part 4 of the *ATA* 2017 makes a series of amendments to CSIS's roles and responsibilities in three significant ways. First, it authorizes CSIS to collect, for the first time, non-threat related personal identifying information to conduct data analytics. The CSIS dataset regime, as it is now known, was a response to a decision of the Federal Court from 2016 that in effect halted all data analytics and dataset collection by the Service for three years, a major blow to any intelligence service operating in the modern threat environment. The history of how CSIS found itself in that position, the mechanics of the regime designed to bring CSIS information collection and big data analytics onto solid legal footing, and the unresolved civil liberties questions raised by the regime are the subject of the first article in this Forum by one of us (Leah West) and Craig Forcese.[18]

The *ATA* 2017's second major reform to the *CSIS Act* is the addition of a long overdue "justification scheme" for CSIS officers and agents who, in the course of their legitimate intelligence collection activities, may need to break the law. In its 2015–2016 annual report, the Security Intelligence Review Committee (SIRC), CSIS's then-review body, noted that CSIS officers and their agents were not protected by the regime established under section 25.1 of the *Criminal Code*,[19] which shields law enforcement from criminal liability when they commit acts or omissions in the course of their duties that would otherwise violate the law.[20] Moreover, SIRC urged that, "CSIS should ensure its employees fully understand the extent to which certain activities present legal risks. To this end, SIRC recommended that CSIS seek legal clarification on whether CSIS employees and CSIS human sources are afforded protection under the Common Law rule of Crown Immunity."[21] The new *CSIS Act* justification scheme resolves this issue and also makes clear that CSIS employees, or those acting under their direction, are not criminally culpable for making false statements or relying on false documents to protect a covert identity.[22]

Finally, the amended *CSIS Act* sets out a detailed process for authorizing other violations of law and the *Charter* by CSIS employees and sources to reduce threats to the security of Canada,[23] a topic addressed by one of us (Michael Nesbitt) in the third article in this Forum.[24] Under Bill C-51, Parliament amended the *CSIS Act*, giving CSIS the authority to engage in "threat disruption measures" or "TRMs." The amendment became so controversial that the threat reduction powers in violation of the *Charter* were never used. The *ATA* 2017 did not do away with TRMs, but as Nesbitt outlines, the reforms addressed many (but not all) of the most pressing concerns about the constitutionality of the threat reduction regime. Nesbitt finds that though the *ATA* 2017 regime is a vast improvement over its Bill C-51 predecessor, it may nevertheless run into legal challenges.

Part 5 of the *ATA* 2017 revises the *Security of Canada Information Sharing* [now *Disclosure*] *Act* (SCISA now SCIDA), which was again introduced in 2015 by Bill C-51.

---

18 Leah West & Craig Forcese, "Building Haystacks: Information Retention and Data Exploitation by the Canadian Security Intelligence Service" (2019) 57:1 Alta L Rev 175.

19 See *Criminal Code*, RSC 1985, c C-46, s 25.1.

20 Canada, Security Intelligence Review Committee, *Annual Report 2015–2016: Maintaining Momentum* (Ottawa: SIRC, 2016).

21 *Ibid* at 20.

22 *CSIS Act*, *supra* note 2, s 18.2.

23 *Ibid*, s 20.

24 Michael Nesbitt, "Bill C-59 and CSIS's 'New' Powers to Disrupt Terrorist Threats: Holding the *Charter*-Limiting Regime to (Constitutional) Account" (2019) 57:1 Alta L Rev 233.

SCISA was a laudable initiative aimed at addressing a long-recognized problem regarding information sharing on national security matters between government departments.[25] Nevertheless, in its original form it was replete with technical problems.[26] For the most part the SCIDA fixed — or attempts to fix — those problems. In so doing, it continues to promote inter-departmental information sharing through non-mandatory language while placing limits on when such information can be shared, and when recipient agencies can retain and use the shared information.

Part 6 of the *ATA* 2017 makes technical reforms to the *Secure Air Travel Act*,[27] another legacy of Bill C-51. When first introduced, the *Secure Air Travel Act* was not terribly controversial, at least as compared to some other aspects of Bill C-51. But in creating a "no fly list,"[28] the *Act* reportedly led to as many as 100,000 people,[29] many of them young children, wrongly identified and forced to undergo additional screening without any form of recourse.[30] For years, unable to get their names removed from the list, the "No Fly List Kids" either could not travel, or had great difficulty when travelling by air. Not surprisingly, the technical amendments introduced in the *ATA* 2017 received bipartisan support; however, it may be years before the modified Passenger Protect Program is fully operationalized.[31]

Part 7 of the *ATA* 2017 reforms the *Criminal Code's* terrorism advocacy offence found in section 83.221 of the *Criminal Code*.[32] The terrorism advocacy offence was introduced by Bill C-51, *An Anti-terrorism Act, 2015*. At that time, it read:

> 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.[33]

The advocacy offence was met by a good degree of controversy and criticism. Kent Roach (along with his collaborator, Craig Forcese) was one of the most outspoken critics of the new provision, stating in no uncertain terms that it was near impossible to discern the offence's

---

25 See 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 (Ottawa: Minister of Public Works and Government Services, 2010) at 26.

26 For a review of these technical problems, see Kent Roach & Craig Forcese, "Bill C-51 Backgrounder #3: Sharing Information and Lost Lessons from the Maher Arar Experience" (16 February 2015), online: <ssrn.com/abstract=2565886>.

27 SC 2015, c 20.

28 The *Act* actually allowed the Minister to identify people that they believed, on reasonable grounds, would threaten transport security or might commit a terrorist act. See *Secure Travel Act*, *ibid*, s 8.

29 See "100,000 Affected Canadians," online: <noflylistkids.ca/en/100000-canadians/>.

30 Amira Elghawaby, "Children Banned from Flying? Sadly, It's Not That Uncommon," *The Globe and Mail* (8 January 2016), online: <theglobeandmail.com/opinion/children-banned-from-flying-sadly-its-not-that-uncommon/article28059610/>.

31 See Canada, Department of Public Safety, "Improving the Passenger Protect Program," online: <www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/pssngr-prtct/mprvng-en.aspx>.

32 *Criminal Code*, *supra* note 19, s 83.221.

33 See *ibid*, as it appeared on 20 June 2019 [emphasis added]; *Anti-Terrorism Act, 2015*, SC 2015, c 20, s 16. Australia did add an advocacy offence in 2005 (see Kent Roach, "A Comparison of Australian and Canadian Anti-Terrorism Laws" (2007) 30:1 UNSWLJ 53 at 82. See also Canada, Library of Parliament, *Legislative Summary of Bill C-51* by Lyne Casavant et al (Ottawa: Library of Parliament, 2018), online: <lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/LegislativeSummaries/412C51E>), which notes that Australia, France, and the UK had offences for "glorification of terrorism."

scope and meaning and that such "[p]oorly defined speech crimes … do violence to our democratic order."[34] In many ways, the trenchant critique offered by Roach and Forcese was an, or perhaps *the*, impetus for Parliament revisiting the offence in Bill C-59.

The *ATA* 2017 revised and clarified the advocating terrorism offence. It 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.[35]

In the second article in this Forum, Roach returns to this issue, analyzing the meaning and implication of the amended offence.[36] He finds that the reworked advocacy crime, while an improvement, remains unsatisfactory. In the end, Roach offers a compelling case for two alternative and more "coherent" options to the existing advocacy offence. First, Parliament could repeal the advocacy (speech) offence altogether. Second, Parliament could narrow the scope of the offence from one that criminalizes "terrorism offences" to one that criminalizes the promotion and advocacy of "terrorist activities," while also adding various defences that apply to other speech crimes and which have been ruled inimical to their constitutionality.[37]

Finally, Parts 8 through 10 of the *ATA* 2017, respectively, offer consequential amendments to the *Youth Criminal Justice Act*; describe how the review period for the *ATA* 2017 will take place, for example by mandating that a comprehensive review be undertaken by a committee of the House of Commons or Senate within four years of the *ATA* 2017 coming into force;[38] and then detail the complex process for the coming-into-force of the *Act*.

Despite the scope of the amendments introduced in the *ATA* 2017, there is much left to be done in terms of national security law reform in Canada. With a view to one of the most salient, and surely controversial, issues left unaddressed by the *Act*, in the final chapter in this Forum, Robert Diab tackles the controversies and debates around proposed government powers to compel decryption of electronic devices.[39] Diab focuses in particular on police powers to compel individuals on arrest or detention to decrypt password-protected cellphones or computers.

(SOME OF) THE OVERARCHING THEMES AND LESSONS OF THE FORUM

The *ATA* 2017 profoundly alters Canada's national security landscape and, in so doing, tackles a host of pressing national security issues, many of which had been left unaddressed

---

34 Kent Roach & Craig Forcese, "Bill C-51 Backgrounder #1: The New Advocating or Promoting Terrorism Offence" (3 February 2015) at 5, online: <www.ssrn.com/abstract=2560006>.

35 *ATA* 2017, *supra* note 1, Part 7, s 143. Subsection 2 clarifies that the offence may be committed even if the person counseled to commit a terrorist offence does not actually do so.

36 Kent Roach, "Terrorist Speech Under Bills C-51 and C-59 and the Othman Hamdan Case: The Continued Incoherence of Canada's Approach" (2019) 57:1 Alta L Rev 203.

37 See for example the Supreme Court's review in *R v Keegstra*, [1990] 3 SCR 697 at 778–80 of Canada's hate speech offence under section 319 of the *Criminal Code*.

38 See *ATA* 2017, *supra* note 1, Part 9, s 168(1).

39 Robert Diab, "The Road Not Taken: Missing Powers to Compel Decryption in Bill C-59, Ticking Bombs, and the Future of the Encryption Debate" (2019) 57:1 Alta L Rev 267.

for decades. Nonetheless, the *ATA* 2017 is doubtlessly imperfect; simply because it addresses needed reforms does not mean that it does so in the most efficient or constitutionally compliant fashion. What can be said is that its many authors seriously considered the legal dubiousness of many of Bill C-51's inventions, and undertook meaningful engagement in an effort to find a balance between the civil liberties of Canadians and Canada's national security imperatives.

The articles in this Forum offer a glimpse into the provenance of some of the most controversial amendments in the *ATA* 2017, how these amendments alter (in some cases fundamentally) the shape of Canadian security agencies, and whether the legislation accomplishes the stated objectives of lawmakers. In so doing, two core themes emerged from these pieces.

First and foremost among these themes is the increasing pace of change in the modern national security landscape and the speed with which the threat environment evolves and adapts. Technological advances in data storage and analytics, encryption, connectivity, and machine learning present new opportunities and new challenges for state actors working to reduce threats to Canadian security. That same technology has the capacity to exacerbate and obfuscate new threats. Together, these advances can pose tremendous risks to the rights and security of everyday Canadians.

As a result, the legal reforms offered in the *ATA* 2017, as evidenced by West and Forcese's article on the collection of datasets by CSIS, are technical and complicated. Those charged with interpreting and applying the law will need to be cognizant of how frequent changes in technology may broaden or narrow the scope of legally permissible conduct. Tenuous legal interpretations may arise when laws crafted with one form of technology in mind are stretched to authorize the use of new tools or forms of collection never contemplated at the time of drafting. Legal reform will never match the pace of technological evolution. That said, we no longer have the luxury of allowing three decades to pass before updating our laws. The goal for the future must be regular, and routine, review and revision of Canada's national security laws, specifically as it relates to information collection, retention, and analysis; it should definitely not proceed as massive and infrequent overhauls of a system on the verge of failure.

The second theme that presents itself in these articles is the increasing role of the judiciary and independent bodies (such as the NSIRA and IC), a product of the broader trend of the legalization of national security in Canada. As West and Forcese note explicitly, and Nesbitt and Diab both imply, with great power comes great responsibility; the *ATA* 2017 attempts to match that power with heightened oversight and review. However, the effectiveness of NSIRA, the IC, and even the Federal Court in providing meaningful review and oversight will depend almost entirely on the capacity and capabilities of their members and staff. These bodies must be adequately staffed and resourced. Failure in that regard risks turning these bodies into a rubber stamp, jeopardizing not only the rights of Canadians but the constitutionality of a number of the regimes introduced by the *ATA* 2017.

Moving forward, it is imperative that academics and concerned citizens keep a close watch on the new powers created by the *ATA* 2017 in order to ensure that they are indeed

exercised with great responsibility. To do so, we need people to watch the watchers—the courts, the NSIRA, the IC, and others—both to keep up-to-date with a proliferation of new practice and review-body reporting, but also to ensure these review and oversight bodies remain up to the task. This all makes for a very exciting time to study national security law and policy in Canada. But it also means that now, more than ever, Canadians are in need of more new, fresh eyes from diverse backgrounds to perform this unofficial oversight role — to hold government to account not just to the rule of law, but to its imperative of keeping Canadians safe. As much as any field in Canada, national security law would benefit from more voices, with diverse cultural backgrounds and ranges of technical expertise, engaging respectfully in debate. We sincerely hope that this Forum forms the impetus for just this sort of debate in the years to come; we hope that it brings more people to the study of national security law in Canada.

[*this page is intentionally blank*]