A declassification strategy for national security and intelligence records

By Wesley Wark

Foreword by Caroline Maynard

As the Information Commissioner of Canada, my role is to investigate complaints about how federal institutions process and respond to requests under the *Access to Information Act*, Canada's freedom of information legislation. In addition, part of my mandate is to give advice and information to parliamentarians and provide arms-length oversight of the federal government's access to information practices, while working with institutions to ensure they meet their obligations under the Act.

Last year, I was invited to organize and host a panel at the May 2019 Open Government Partnership (OGP) Summit in Ottawa. This panel, entitled *Declassification of Government Records: A Way Forward Towards Improving Transparency*, brought together leading experts from the United Kingdom, the United States, as well as Library and Archives Canada to discuss a topic that, while not central to my mandate, is one that interests me. This is primarily because the lack of a *de-classification* system in Canada has had an increasingly significant impact on my office's work.

My office currently has an inventory of over 5000 complaints. Almost 20% of this workload involves complaints related to national security-related information sought through access to information requests. Of this, our refusal investigations, where we review the reasonableness of the searches conducted, or the appropriateness of the exemptions applied, total about 45,000 pages of classified information. However, we have been told that other records related to administrative investigations, where the government hasn't yet responded to the access requests, could potentially represent additional millions of pages of classified documents. In short, the task involved in investigating these types of file is immense.

Under a proper system of declassification and review of historical national security and intelligence-related records, many of these files would have been declassified and sent to our national archives, and would now be accessible to researchers and others who seek access to them. But, because Canada lacks such a declassification regime, they remain at the original institution, inaccessible to all, except through an access to information system ill-suited to this specific purpose. I was therefore keen to start a conversation and generate ideas on how Canada could go about addressing this challenge.

Following the panel, which featured some interesting exchanges between the panellists comparing the frameworks in which they operate, Professor Wesley Wark from the University of Ottawa, who attended the session as rapporteur, wrote the paper that follows. It lays out some proposals for a possible declassification strategy for national security and intelligence records and represents a possible path forward for Canada.

I would like to thank the panellists who participated in the session, whose names are listed below. Their contributions that day kick-started a discussion that I hope will continue in the months to come.

I am pleased now to share this discussion paper with you and I encourage you to consider the recommendations contained therein. My priority will be to address Recommendations 1, 3 and 13 as I believe they have the most direct and immediate impact on the access to information system. It is through collaboration and a collective commitment to openness that trust in democracy and our institutions can flourish. Let us consider the ways in which we can contribute to maximum success.

Panelists at the OGP session on declassification of government records, "A Way Forward Towards Improving Transparency"

Paulette Dozois

Senior Lead Archivist/Block Review Team Leader
Library and Archives Canada

Daniel German
Senior Archivist
Library and Archives Canada

Nate Jones
Director of the Freedom of Information Act Project
National Security Archive
George Washington University

David J. Mengel
Deputy Director
National Declassification Centre
US National Archives

Malcolm Todd
Head of Policy
The National Archives, UK

1. Why declassification matters?

Canadian national security policy in the years since the 9/11 attacks has rested on an understanding of the need to ensure democratic practices while protecting Canada against threats to our democracy. This message was contained in the first-ever National Security strategy published by the Canadian Government in April 2004. It included statements such as the following:

"The Government needs the help and support of all Canadians to make its approach to security effective…"

"We also need to ensure that there are effective mechanisms for oversight and review so that, in protecting an open society, we do not inadvertently erode the very liberties and values we are determined to uphold." [1]

More recent official statements on national security and intelligence policy extend these sentiments by explicit recognition of the need on the part of the security and intelligence community to be more transparent and open about their practices in order to ensure that they have the support and understanding of Canadians.

In a speech delivered by the CSIS Director, David Vigneault, in Toronto in December 2018, this linkage was directly expressed:

"We're also aiming to be more transparent about our work – to the extent that we can be, given our line of work. By engaging Canadians about the threats we're facing, we hope to make them our partners in building protections against these threats."[2]

In a similar vein, the then Minister of Public Safety, Ralph Goodale, explained the rationale for the government's announcement of a National Security Transparency Commitment, by noting that:

"Canadians must know what the Government does to protect national security, how the Government does it, and why it's important. Providing information to Canadians on what the government does to protect their national security is essential to demonstrate that their values are being upheld." [3]

Without striving for that quantum of democratic legitimacy, the prospect arises of democratic divides, loss of public support, weakening political engagement with the intelligence community, internal morale problems within security and intelligence

[1] Privy Council Office, Securing an Open Society: Canada's National Security Policy, April 2004, archived

[2] CSIS, David Vigneault speech, The Economic Club of Canada, Toronto, December 10, 2018

[3] News release, Minister of Public Safety, July 2, 2019

agencies, and even the rise of security practices that abuse Canadian norms and laws.

Political promises and commitments in support of sustaining public knowledge are set in the context of raised public awareness and interest in Canada regarding national security and intelligence matters, which itself is rooted in a new security environment and profound change that has occurred since the 9/11 attacks.

Allowing Canadians better access and understanding of the history of Canada's national security and intelligence practices is one important path to ensuring the goals of democratic accountability, transparency and legitimacy. Creation of a strong historical memory requires new approaches, especially to the declassification of significant historical records regarding Canadian national security and intelligence promises many potentially important benefits. A strong declassification strategy for national security and intelligence records should be seen as a contributor to the goals of accountability, transparency and democratic practices as well as offering performance enhancing benefits to the security and intelligence community itself.

The declassification and public release of significant, historic records on Canadian national security and intelligence, in addition to making a general contribution to the drive for open government, transparency and accountability, offers some more specific potential benefits:

- Sustaining the collective memory of the government security and intelligence community
- Offering evidentiary lessons-learned records to help improve performance
- Assisting in recruitment and training of new entrants to the federal security and intelligence community
- Sustaining ethical, legal and cultural norms within the security and intelligence system
- Helping educate the Canadian public about the nature, necessity and challenges of a security and intelligence system
- Helping sustain a broad public consensus about the need for a sovereign intelligence system to support Canadian security requirements in keeping with Canadian values
- Filling in the "missing dimension" of our historical understanding of the role of Canadian intelligence in supporting Canadian foreign, defence and national security policy

In addition to these principled benefits there could be an important practical outcome for the work of the Office of the Information Commissioner. Significant progress on declassification of historical national security and intelligence records could benefit the work of the OIC through lessening of pressure on the access system and complaints process, allowing for maximum use of the Office's resources, and maintenance of the integrity of the *Access to Information Act* (ATIA) regime.

The Office of the Information Commissioner, with a mandate to investigate complaints regarding access to information requests and to maintain oversight over the *Access to Information Act* regime, can play a key role in helping both the federal Government and Canadians realize some of these principled and practical benefits, especially in the context of the coming debate over a full scale review of the ATIA, scheduled to begin in the summer of 2020.

2. A quick look back on access

Prior to the creation of Canada's first *Access to Information Act*, the public release by the federal government of information under its control was entirely a discretionary matter. There were provisions in place, through Cabinet directives, for the classification of government recordings (security markings), first made public with the *1969 Report of the Royal Commission on Security*, and for declassification of almost all Federal governments records after thirty years—the "Thirty Year rule" and their transfer to the National Archives (as it then was), but no promise of systemic public access. This declassification and transfer practice was spelled out in Cabinet Directive 46, approved in June 1973. The principle of administrative secrecy remained uppermost.[4]

The global advance of freedom of information legislation, particular the passage of the US *Freedom of Information Act* (FOIA) in 1966 spurred interest in creating a similar statute in Canada. Advocacy in Parliament led the government to produce a Green paper in June 1977 discussing options for a Canadian FOIA. An Access bill and a Privacy bill were introduced in Parliament in July 1980.[5]

The *Access to Information Act* was subsequently passed by Parliament, and given Royal Assent in 1983. One provision of the Act called for a comprehensive review to be commenced within three years of its enactment, an unusual requirement in its day. The Standing Committee on Justice and the Solicitor General conducted the review and issued its report in March 1987, entitled "Open and Shut: Enhancing the Right to Know and the Right to Privacy."[6]

One chapter of the Committee's wide-ranging report zeroed in on the exemptions regime—it called exemptions "perhaps the most crucial part of any access to information system…" It called for major revisions in the drafting of exemptions in the Act, saying this was considered "vital for the credibility of this legislation." The Committee's recommendations were that all exemptions should be discretionary, and should be based on a reasonableness standard of harm, which should be

---

[4] Library of Parliament, David Johansen, "Public Access to Federal Government Information, " Current Issue Review 79-5E, 15 August 1979, revised 30 July 1982

[5] *ibid*

[6] House of Commons, Report of the Standing Committee on Justice and Solicitor General on the Review of the *Access to Information Act* and the *Privacy Act*, March 1987

defined as "significant injury."[7] These recommendations were prescient in identifying real and persistent problems with the access legislation but were not taken up by successive governments, down to the present.

Fifteen years later, a Treasury Board task force was constituted to do its own review of the access to information regime. The task force, chaired by Andrée Delagrave, and consisting of members drawn exclusively from federal government departments and agencies, submitted its report in June 2002.[8] While it was constituted just before the 9/11 attacks, its report was completed in the aftermath of major changes to the national security and intelligence environment forced on Canada.

The task force took a cautious and deferential approach to the question of exemptions and the declassification of records, perhaps not surprising given the times and the membership of the group. It rejected expert advice from external stakeholders and its own commissioned studies, which argued for the re-imposition of a time expiry rule on declassification and transfer of records, and did not consider that sensitive records would necessarily be of less sensitivity over time, even after the passage of 30 years. While it supported the idea of bulk review of historical records based on an understanding of historical context and what it called "educated risk management," the Task Force would go no further than suggesting that the National Archives play a leading role in developing a system for bulk review. The task force acknowledged that an initiative for bulk review would require additional resources.[9]

With regard to the powers of the Information Commissioner, the Task Force did recommend that the Commissioner should have a public education mandate about the ATIA, that the Information Commissioner should publish case summaries of access requests on an ongoing basis, that the Information Commissioner should have an explicit mandate to advise government institutions on new legislation, policies and directives, on the administration of the Act and on best practices.[10]

All of these recommendations would have extended the role of the Information Commissioner, but none have yet been baked into ATIA reform.

But pressure for change has persisted. One notable development involved a major Federal Court ruling.[11] The Federal Court heard a complaint instituted by Jim Bronskill of the Canadian Press into the handling of redactions of the security file on the former Canadian politician, Tommy Douglas. Senior Federal Court judge, Simon

---

[7] *ibid*. See Chapter 3 of the report, "Exemptions and Cabinet Confidences: Saying No," especially pp. 19-20

[8] Government of Canada, Access to Information Review Task Force, Access to Information: Making it Work for Canadians, June 2002. Archived

[9] *ibid*, Chapter 8, "Meeting the Information Needs of Canadians Outside the *Access to Information Act*, pp. 138-140

[10] ibid, chapter 6, "Ensuring Compliance: The Redress Process," on the Mandate of the Information Commissioner, pp. 92-96

[11] *Bronskill v. Canada (Canadian Heritage)*, 2011 FC 983 (CanLII), [2013] 2 FCR 563 h

Noël, in adjudicating this complaint had many important things to say, in a nearly 100 page ruling, about handling of access requests of formerly sensitive national security files.

Justice Noël commented on the need for a declassification process for historic records, for an understanding of the benefits of public access to historic records, an appreciation of the reality of declining sensitivity over time of national security records, and the need for a better exercise of discretionary judgment over the release of historic and significant records, particularly in the context of applying the national security exemption found at section 15 of the ATIA.[12]

More calls for change have followed in recent years. In March 2015, in a special report submitted to Parliament, entitled "Striking the Right Balance for Transparency: Recommendations to Modernize the *Access to Information Act*", the then Information Commissioner, Suzanne Legault, called for an overhaul of the exemptions regime, arguing that a model system would feature exemptions that are:

- Injury based
- Discretionary
- Time-limited
- Subject to a public interest override
- Subject to independent oversight [13]

Some interim reforms have been enacted. The government introduced revisions to the ATIA in June 2017 (Bill C-58), which were eventually made into law in June, 2019.[14] However, Bill C-58 did not undertake to amend any of the exemptions in the Act, nor did it introduce provisions regarding declassification or transfer of records. More substantial change will have to wait on the completion of the promised full review of the ATIA.

As the current Information Commissioner, Caroline Maynard, has suggested to Senators, there is much that we can learn from the history of our engagement with the ATIA going back to 1983, and the past studies and reform suggestions that have been advanced.[15] This material should be well utilized in any future full review of the ATIA. The OIC is excellently placed to be a central resource for ensuring that this past history of efforts to learn lessons from the Act and to make it more fully compliant with its underlying democratic accountability objectives are not forgotten.

---

[12] *ibid*

[13] Office of the Information Commissioner, Special Report to Parliament, Striking the Right Balance for Transparency: Recommendations to Modernize the *Access to Information Act*, March 2015, See especially Chapter 4: Maximizing Disclosure"

[14] Bill C-58, An Act to Amend the *Access to Information Act*...; See also the Library of Parliament Legislative Summary of Bill C-58, publication no. 42-1-C58-E, revised August 1, 2018

[15] Testimony of the Information Commissioner of Canada on Bill C-58, before the Senate Standing Committee on Legal and Constitutional Affairs, October 17, 2018

3. An opportune time?

The issue of the declassification of records, and the disposition of historically significant records, is rarely front and centre in discussions of open government practices, transparency principles, and the function of the access regime.

This is the case despite the fact that national security and intelligence records sit at the very heart of the core tension between the broad principles of access to information first set out when access legislation entered the statute books in 1983, and the need to protect sensitive information in the furtherance of security policy. The fate of national security and intelligence records is, arguably, the thorniest problem facing the Canadian access to information regime and one that we have failed over the past 35 plus years to satisfactorily resolve.

The Information Commissioner's Office is directly affected by this unresolved problem. In opening remarks for a panel on "Declassification of Government Records" held at the recent Open Government Partnership Global Summit in Ottawa, the Information Commissioner, Caroline Maynard, noted that her office, at that time, was dealing with an inventory of 3,600 complaints regarding information disclosure under the *Access to Information Act*. Fully twenty percent of this total relates to records containing national security information (c. 720 complaints).[16]

Ms. Maynard indicated that of these, there are 110 complaints currently under investigation by her Office into redactions of records with historical national security content (i.e., records that have already been transferred to Library and Archives Canada, or should have been, as they are of archival, rather than operational, value).[17] Each of these complaints investigations can be complex, time-consuming and resource intensive, with outcomes that are inherently unpredictable.

The Information Commissioner made the point in her remarks that Canada does not have a real strategy for declassification of national security records.

Achievement of such a strategy would benefit the work of the Information Commissioner's office, by alleviating pressure on the complaints system, would strengthen the access to information regime, not least by reorienting thinking on records secrecy and the application of exemptions under the Act, and would contribute to government priorities regarding open government, transparency, and democratic legitimacy with regard to national security practices.

A confluence of circumstances suggests that there is an opportunity to raise the profile of this problem and to seek solutions. These circumstances include the federal government's on-going commitment to open government principles, which crosses party lines; its engagement in the Open Government Partnership, with the

---

[16] Speaking notes prepared for the Information Commissioner, "*De-classification* of Government Records: Supporting Democracy and Renewing Trust," Delivered May 31, 2019, copy courtesy of the OIC.

[17] *ibid*

reporting and public consultation practices this entails; the recent passage of revised access to information Legislation, including order-making powers for the Information Commissioner; the promise of a full scale review of the *Access to Information Act* to commence no later than June 2020; the federal government's commitment to national security transparency, first outlined in June 2017; the desire of security and intelligence agencies to increase public knowledge of their work through transparency initiatives; and indications, especially in the form of responses to the Government's 2016 Green paper on National Security, of renewed public pressure for greater transparency around national security and intelligence, including the historical record.

As the President of the Treasury Board stated in late May 2019 in written response to a petition presented to Parliament, the government has legislated important changes to the *Access to Information Act*; has committed to proactive disclosure of government records (the "open by default" principle); and will embark on the first full review of the *Access to Information Act*. The TB President, in her letter, committed to continuing to work with "Parliamentarians, the Information Commissioner and Privacy Commissioner, indigenous groups and other stakeholders to further strengthen government openness and transparency, including in the first full review of the Act."[18]

The Office of the Information Commissioner will play an important role in the review and has an opportunity to seed the debate with, among other things, concrete proposals for advancing the systemic declassification of government records, especially those dealing with national security and intelligence.

4. Leveraging the National Security Transparency Commitment

The National Security Transparency Commitment was made public in combination with the introduction of the National Security Framework Legislation, Bill C-59, in Parliament in June 2017.[19]

Beyond the initial June 2017 statement of the six principles that will drive the commitment, there is little public information available about how national security transparency will be delivered in practice.

The NS Transparency Commitment is being managed by a small team at Public Safety. A senior official at Public Safety (Associate Deputy Minister Dominic Rochon) now serves as co-chair of an advisory committee on national security transparency, hopefully signaling a desire to move the commitment forward.

---

[18] House of Commons, Response by the President of the Treasury Board to Petition no. 421-03899 [Murray Rankin], May 27, 2019

[19] Public Safety Canada, National Security Transparency Commitment

Despite the passage of over two years and the absence of public information about implementation, the national security transparency commitment may still hold promise. Its enunciated principles can be considered a potential lever in addressing declassification initiatives with regard to national security records.

There are two reasons for considering the commitment as a potential lever. One is provided by the general rationale supporting the commitment, which reads:

"…citizens must know what the Government does to protect national security, how the Government does it, and why such work is important."

While this rationale is conveyed in the present tense, with the implication that the commitment is all about current national security policy, the six principles go beyond the **presentism** conveyed by the rationale.

It can be argued that specific principles among the six enumerated give the commitment both a historical and a forward leaning dimension. In particular Principle 2 on information transparency holds promise.[20]

It reads:

"Departments and agencies will enable and support Canadians in accessing national security related information to the maximum extent possible without compromising the national interest, the effectiveness of operations, or the safety or security of an individual."

These caveats are, of course, open to interpretation. Further (minimal) clarification provided in the statement on the Transparency Commitment indicates that:

"Information should only be treated as sensitive when Canada's interests are at stake—where disclosure could harm national security or our relations—or personal information is included."

While this exclusionary argument broadly aligns with the exemption regime under access, it can still be argued that the spirit of the NS Transparency Commitment offers an opening. Principle Two could be deployed to support the case for a systemic declassification and release process for historical records dealing with national security and intelligence, in line with broader arguments that public access to historical records is a significant part of delivering democratic accountability.

5. The Open Government Action Plan: Reality and potential

Canada developed its first "Open Government" strategy under the Conservative Government of Stephen Harper in 2011, and joined the Open Government Partnership (OGP) in April 2012. Membership in the OPG requires states to produce

[20] ibid, Principle Two

action plans on a biannual basis, addressing structured commitments under one or more of the OGP's "grand challenges." The Canadian government has produced a series of such plans, the first covering the years 2012-2014. The most recent, issued in December 2018 following public consultations, spans the years 2018-2020.

Commitments regarding access to information reform and the declassification of federal records are sprinkled throughout the successive action plans, which are generally very broad ranging in scope. None of the action plans to date specifically refer to national security and intelligence records and their declassification.

The first action plan (2012-14) talked about increasing access to records held by LAC and removing restrictions on access to these records "wherever possible." It also promised to issue new mandatory policy on consistent document classification procedures "to reduce the volume of classified documents in the future." The Action Plan also promised measures "to progressively make the classified documentation already held within the archives of the Government of Canada available online…"[21]

The second action plan (2014-16) repeated some of the commitments made previously around improving the efficiency of the access system and better enabling access to archived federal records. It committed the government to proactive release of data and information, which it called "the starting point for all other open government activities." The second action plan promised the creation of a "new online virtual library to preserve and improve access to historical and archival records."[22]

In commenting on the 2014-2016 Action Plan, the then Information Commissioner, Suzanne Legault, urged a systemic declassification process for government records.[23]

In the OGP mandated end-of-term progress report for 2014-16, an emphasis was placed on the lessons that had been learned to date in delivering on Open Government commitments. The key lessons outlined in the first self-assessment report included the need for strong public engagement, the importance of establishing guidance and standards that federal government agencies could follow in developing open government initiatives, and the obstacles created by limited financial and human resources. There was also a dawning realization in the OGP progress report—"we learned that the amount of cultural and process transformation needed within the Government of Canada's working environment is greater than originally thought."[24]

The third action plan (2016-2018) included commitments to review *the Access to Information Act* under a two-stage process, and to create a new Cabinet Committee

---

[21] Canada's Action Plan on Open Government 2012-2014
[22] Canada's Action Plan on Open Government 2014-2016
[23] Letter by the Information Commissioner to the President of the Treasury Board on Canada's Action Plan 2.0, November 5, 2014. Copy courtesy of the OIC.
[24] End-of-Term Self-Assessment Report on Action Plan on Open Government 2014-2016

on "Open and Transparent Government."[25] The full review of the ATIA has been delayed until a start date of summer 2020, two years later than originally planned. This review follows the Royal Assent given to Bill C-58, to amend the Access to Information Legislation, in June 2019.

The Cabinet committee was of relatively short duration, merging with the Committee on Parliamentary Affairs in August 2016 and then disappearing altogether from the list of committees with a re-structuring in August 2018.

As action plans grew in size and with a corresponding increase in commitments (22 in total for the 2016-2018 action plan), so did the size of end of term self-assessment reports. The self-assessment report for 2014-2016 was five pages in total; that for 2016-2018 was sixty-five pages.

The end of term assessment report for 2016-2018 included a reference to reform of the ATIA, noting that:

"the Government of Canada is committed to modernizing the Access to Information Act. This is a complex task. In preparing new legislation and trying to respond to stakeholder input, we were reminded again that changes to the Act need to be crafted carefully to balance more open government with other important democratic values, such as the privacy of citizens, the impartiality and objectivity of the public service, and the independence of the judiciary."[26]

It may be noted that no reference was made here to the need to balance open government objectives with security considerations, as the Act is "modernized."

The end of term report for 2016-2018 also commented on Library and Archives Canada's block review initiative, noting that it involved the review of more than 11 million pages of archived government records and the opening of 10.5 million of those pages. No mention was made of the fact that block review excludes from its purview national security and intelligence records.[27]

The most recent version of the Open Government Action plan is for the years 2018-2020. Once again, the Government advances a broad range of commitments (10 in number), arguments in their support, and delivery plans.[28]

While there is, in keeping with previous action plans, no specific mention of national security and intelligence records, there is a discussion of a commitment to improve the ATIA (commitment 7). Among the elements of this commitment are the reiteration of the promise to undertake a full review of the ATIA starting one year after Royal assent to Bill C-58, the interim amendments to the ATIA. Among the promises made are that the review will include a consideration of the regime of

---

[25] Third Biennial Plan to the Open Government Partnership (2016-2018)

[26] End-of-Term Self Assessment Report on Canada's Third Biennial Plan to the Open Government Partnership 2016-2018

[27] *ibid*

[28] Canada's 2018-2020 National Action Plan on Open Government

exemptions and exclusions, will look at ways to improve timeliness of responses to requests, and will explore the potential of new technologies to assist in ATIA delivery.

In a letter to the President of the Treasury Board on the 2018-2020 Action Plan, the Information Commissioner expressed some disappointment, "with the limited scope of the commitments in the Plan related to access to information, and whether they reflect your government's open government agenda." As co-chair of the OGP Steering Committee, she encouraged the Government "to be more ambitious in its commitments and to show real, transformative leadership on this front."[29]

The Open Government action plan process can be important for setting out priorities, for its promise of public engagement, and for trying to measure progress. Successive action plans and self-assessment reports can also easily dissolve into rhetoric. The OPG-derived format of bi-annual reports and specified commitments related to externally set "grand challenges" can impact beneficially on both longer-term planning and on overall strategic direction, but only if commitments are acted on.

The Open Government action plan could be a potential platform in future for specific calls to action with regard to the treatment of national security and intelligence records. For this to happen, national security and intelligence issues need to penetrate discussions at the OGP in a systematic way. This could have an important knock-on effect for the internal debate in Canada.

6. Treasury Board directives impacting on declassification of national security and intelligence records

On July 1, 2019 the Treasury Board instituted a new "Directive on Security Management."[30] This Directive replaced a number of previous directives and security standard documents. The new directive has important and worrisome implications for the declassification of national security records and would appear to be philosophically at odds with the thrust of other government policy, notably the national security transparency commitment.

To understand these worrisome implications, one has to compare the new directive with the "Security Organization and Administration Standard," a TBSpolicy that operated between June 1, 1995 and July 1, 2019.[31]

---

[29] Information Commissioner of Canada, letter to the Honourable Scott Brison, President of the Treasury Board, September 18, 2018, copy courtesy of the OIC

[30] Treasury Board Secretariat, Directive on Security Management, July 1, 2019

[31] Treasury Board Secretariat, Security Organization and Administrative Standard, rescinded June 28, 2019

The new directive employs barebones, "where appropriate," language to address issues of downgrading security markings on documents, indicating that the security category applied to a records may be downgraded "when the expected injury is reduced." It also discusses upgrading the security classification on a record when the expected harm is increased.[32]

There is no guidance provided in the new directive regarding automatic declassification, the handling of access requests, transfer of records to Library and Archives Canada, or any special circumstances surrounding systemic review of records held by CSE and CSIS for the purposes of declassification or downgrading of classified information.

All of this is in distinct contrast with the superseded Security Organization and Administration Standard (1995-2019), which contained guidance on all these issues.

In particular the new Directive fails to carry over the language of the old Standard with regard to recognition of the loss of sensitivity of records over time, a vital construct supporting declassification. The previous standard stated:

"Information must be classified or designated only for the time it requires protection, after which it is to be declassified or downgraded."[33]

The previous Standard explicitly recognized two important factors:

a. that classified information will lose its sensitivity over time
b. that the process of declassifying records that have lost their sensitivity with the passage of time "contributes to the overall integrity of the security system, and ensures that information is made available quickly and informally to interested members of the public."[34]

It is a moot point that the old Standard may never have produced the outlook or effects it sought, but the absence of such guidance in the new Directive contributes a significant obstacle to change.

The new Directive also fails to reproduce the guidance contained in the old Standard on automatic declassification, with its reference to a 10-year trigger for records marked at the secret or lower levels.

To compound matters, the new Directive also scrubs previous language about the handling of access requests, which contained the reminder that the withholding of all or parts of a record in response to an ATIP request "*must be based solely on the*

---

[32] Treasury Board Secretariat, Directive on Security Management, section E.2 at E.2.2.2.2
[33] Treasury Board Secretariat, Security Organization and Administrative Standard, rescinded June 28, 2019, at 12.1
[34] Treasury Board Secretariat, Security Organization and Administrative Standard, rescinded June 28, 2019,

exemption provisions" of the Act and must not be based on security markings of the record itself.

Instead the new Directive muddies the waters by stating that:

"From a Confidentiality standpoint, the security category for information considers the exemption and exclusion criteria of the *Access to Information Act* and the *Privacy Act* to ensure that resources are not applied to protected information that can be made public."[35]

Nor is there any guidance in the New Directive with regard to the need for departments to review their information classification guides in the light of periodic reviews of outcomes of ATIP requests.

The new Directive also drops any reference to the need for departments to develop agreements with LAC "to declassify or downgrade sensitive information transferred to the control of the Archives."

Altogether, the new Directive manages to achieve a significant weakening of incentives for the declassification and release of historic national security records. The new Directive thereby runs counter to the acceptance of open government principles, reform of the *Access to Information Act*, the commitment to national security transparency, and the over-arching appreciation of the need to maintain public legitimacy for national security activities.

The impediments that the new TBS Directive presents with regard to access to historic national security records should be part of the forthcoming full review of the ATIA.

7. The *Library and Archives Canada Act* and the *Access to Information Act*: Pathways and problems for declassification

Two major statutes—the *Library and Archives Canada Act* and the *Access to Information Act*—govern the public disposition of federal government records.

The *Library and Archives Canada Act* dates to 2004 when the Archives and the National Library were combined in one.[36] The Act is relatively brief. Its preamble refers to the function of the LAC as "the continuing memory of the government of Canada" and a source of "enduring knowledge accessible to all."

The key provision of the LAC Act that illuminates the current practice of the transfer and declassification of records is **subsection 13(1)** which states:

---

[35] Treasury Board Secretariat, Directive on Security Management, Appendix J at J.2.2.6

[36] *Library and Archives of Canada Act*

"The transfer to the care and control of the Librarian and Archivist of government or ministerial records that he or she considers to have historical or archival value shall be effected in accordance with any agreements for the transfer of records that may be made between the Librarian and Archivist and the government institution or person responsible for the records."[37]

There is no stipulation in the Act for a statutory requirement to transfer records, or for a time frame in which records must be transferred.

The Librarian and Archivist has only a loosely worded advisory function with regard to the management of government information, **subsection 8(1):**

"advise government institutions concerning the management of information produced or used by them and provide services for that purpose."[38]

There is no requirement in the LAC Act regarding the mandatory preservation of government records and no powers accorded the Librarian and Archivist in that regard.

If the *Library and Archives Act* is meant to sustain the idea of a national memory bank, the *Access to Information Act* was designed to assist citizens to gain entry to that 'national memory' as a way to sustain and enhance democratic accountability.

The Act was initially promulgated in 1983. A recent set of amendments to the Act was proposed in Bill C-58, which gained Royal Assent in June 2019. The Legislative summary of Bill C-58 prepared by the Library of Parliament provides a useful tracking of the history of the Act and of the revisions enacted.[39]

The wording of the purpose of the Act has now been amended, with Bill C-58, to read:

"The purpose of this Act is to enhance the accountability and transparency of federal institutions in order to promote an open and democratic society and to enable debate on the conduct of those institutions."[40]

The revised Act retains the original wording suggesting that ATIA is meant to:

"complement and not replace existing procedures for access to government information and is not intended to limit in any way access to the type of government information that is normally available to the general public. "[41]

The question of the status and nature of "existing procedures" is not clarified in the statute nor is the concept of "normally available," particularly as it might apply to historical records. What has become clear in the years since the passage of the

---

[37] *ibid*, s13(1)
[38] *ibid*, s8(1)
[39] Library of Parliament Legislative Summary of Bill C-58, publication no. 42-1-C58-E, revised August 1, 2018
[40] Bill C-58, An Act to Amend the *Access to Information Act*…
[41] *ibid*

original ATIA is that the practice of treating the release of records after a specified thirty year period (the so-called "thirty year rule") has been nullified and replaced by the requirement to process all national security and intelligence records through individual and autonomous ATIA requests.

The amendments in C-58 do not fundamentally alter the current practice with regard to the issue of national security and intelligence records or their declassification. Public access to national security and intelligence records remains largely subject to individual ATIA requests and the application of classes of exemptions specified in the ATIA. These classes of exemptions have not been revised since the original passage of the Act in 1983.

The key exemptions relevant to national security and intelligence records include:

Section 13 (information obtained in confidence)

In the Treasury Board "Interim Directive on the Administration of the *Access to Information Act*" (May 5, 2016), the section 13 exemption is classed as mandatory and not based on an injury test.[42] But there is a theoretical discretionary element involved, set out in the *Access to Information Act* at 13(2) that allows for discretionary release when the originating agency consents or makes the information public. Efforts to acquire consent are rarely successful, especially when it comes to security and intelligence records where originator control rests in a foreign service. Disclosure on the basis of knowledge that the originating party has made the information public requires research and knowledge of originating entity practices, which may be curtailed by lack of resources and expertise, again especially with regard to foreign security and intelligence agencies.

Subsection 15(1) (international affairs and defence)

This is another major category of exemption typically applied to national security and intelligence records. It is discretionary and is meant to be based on a harms test.

It states:

"The head of a government institution **may** refuse to disclose any record requested under this Act that contains information the disclosure of which could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities…"[43]

---

[42] Treasury Board Secretariat, Interim Directive on the Administration of the *Access to Information Act*, May 5, 2016

[43] *Access to Information Act* [consolidated]

A number of illustrative examples of what mightfall within the scope of the exemption, subject to the institution establishing the injury described in the opening words of the exemption, are listed in the Act.[44]

Section 21 (advice)

Generally this exemption protects the policy- and decision-making processes of government, including for national security and intelligence policy. It is a discretionary exemption and also, unusually for the Act, carries with it a time limit of 20 years.[45] There is no harms test to be applied, although harm is usually a relevant factor to be considered during the exercise of discretion.

In combination, the exemptions available in the ATIA can amount to a considerable barrier to public access to records and to the "national memory" function of such records, particularly as redactions are applied and atomisation of records occurs through responsiveness to individual ATIA requests.

In considering the current LAC and ATIA legislation in combination, the following problem areas are apparent:

1. the lack of any statutory requirement for the creation and preservation of government records
2. the lack of any time limits for the transfer of federal records to LAC
3. the lack of any time limits on the expiry or downgrading of security markings on records and their public release
4. the lack of any statutory authority for the Librarian and Archivist regarding enforcement of time lines for transfer of records and for declassification powers
5. the deferential nature of exemptions provided under ATIA, which arguably do not require the exercise of a serious harms test, and do not give any directional force to a public interest override or balancing calculation. The practice of applying exemptions does not enforce recognition of the historical significance of records, or the fact of declining sensitivity of records over time. All of these elements should be included in the exercise of discretion but there is no guarantee of how they may be weighted and no real leverage provided to combat the possibility of an excessive practice or culture of secrecy.

In a letter provided to the Chair of the Senate Standing Committee on Legal and Constitutional Affairs during that Committee's consideration of Bill C-58, the Information Commissioner responded to Senators' requests for her opinion on what elements of ATIA should be revised under the promised full review of the Act. The Commissioner's suggestions included giving consideration to a legal requirement to create and preserve records, to efforts to tackle the "culture of delay" in handling access requests, to tighten precision around exclusions applied to Cabinet

[44] *ibid*, at s15(1)(a) through (i)

[45] *ibid* at s21

confidences, and to revisit the long-standing exemptions applied to records under the Act.[46]

Ms. Maynard argued in her letter that:

"Most of the exemptions under the Act are as old as the Act itself and have not received significant review in 35 years. The exemptions do not take into account societal expectations for transparency, modern technology, or current open government practices."[47]

Ms. Maynard also told Senators that:

"The Office of the Information Commissioner has thirty five years' worth of data on how these exemptions are applied and what works, what doesn't work and would be pleased to provide this information during second phase review."[48]

This body of information would be of great value to support an evidentiary approach to reform of the ATIA. That value would be increased if the OIC data is available in synthesized form that allows for analysis of particular aspects of the legislation, for example the application of the subsection 15(1) exemption over time.

More broadly the LAC Act and the ATIA separately, and in combination, fail to recognize the importance of the preservation of a comprehensive and cohesive historical record. The ATIA in fact works to create the opposite, by generating (where it does generate at all) a piecemeal and fractured record of the historical past based on individual record requests. LAC receives and catalogs records in siloed record groups that are fashioned in accordance with individual department and agency repositories.

Putting together a comprehensive historic picture is inherently difficult with reliance on the existing procedures of the LAC and the ATIA. Official histories and the release of special record sets accompanied by a historical narrative could in important ways fill some of these gaps. This practice has been embraced in significant ways by Australia, the US and the UK, our key Five Eyes partners. Possibilities such as this were highlighted in the discussions sponsored by the OIC and chaired by the Commissioner in a special panel held during the OGP Global Summit in Ottawa in May 2019.

8. Learning from best practices

In the past four years, substantial changes have occurred to the review system for the Canadian security and intelligence community, including the creation of a security-cleared committee of Parliamentarians (NSICOP), and the standing up of a

[46] Letter, Information Commissioner to the Honourable Serge Joyal, Senator, Chair, Standing Senate Committee on Legal and Constitutional Affairs, November 1, 2018, p. 9. copy courtesy of OIC.Return to footnote referrer46

[47] *ibid*

[48] *ibid*

new National Security and Intelligence Review Agency and the creation of oversight powers for a new Intelligence Commissioner. These changes were rooted in political debate around national security policy in Canada, and recognized that the Canadian system of national security and intelligence review had failed to keep up with the times, or match its early promise of situating Canada as a world leader among democracies. The changes were embedded in new legislation passed in 2017 and in 2019 (Bills C-22 and C-59 respectively).

The prospect of similar advances in Canada's access to information regime, which shares an origin date close to the first attempts at security review in Canada (the CSIS Act of 1984 which created the original Security and Intelligence Review Committee) will require the same set of stimuli—strong political debate; and a recognition of a model that has grown stale, outdated and which fails to sustain Canada's place as a global leader.

In considering new structures, policy and legislation for national security and intelligence review, the government paid especial attention to best practices and the experience of our close intelligence partners in the Five Eyes (US, UK, Australia and New Zealand) and NATO. The legislation that created the National Security and Intelligence Committee of Parliamentarians was closely modeled on similar legislation in the UK, which created the Intelligence and Security Committee. Review practices in the Five Eyes community were mined in the creation of the new review and oversight bodies set out in Bill C-59.

At the same time, the government was clearly bent on creating a new national security and review system which would be ambitious, innovative and capable of being hailed as a global leader.

A similar spirit should animate current and future discussion on changes to the access to information regime. Similarly, learning from the best practices and experience of our partners in the Five Eyes will be important. Our Five Eyes partners are all democracies with versions of Freedom of Information Legislation, and commitments to maintain a living archive of government records accessible to the public. All have struggled with ways to ensure the declassification and transfer of records to national repositories, and all have endeavoured to find the right balance in their access/freedom of information systems between the principles of ensuring public access to records and the need to protect security.

A detailed examination of best practices among our Five Eyes partners is beyond the scope of this present paper. OIC officials have some familiarity with the regimes that govern records among our allies. This could be built upon in collaboration with federal government departments and agencies.

It is clear that recent changes to practice by our allies warrant close attention in Canada, to see what we can learn and apply in a Canadian context. Of these changes three will be briefly highlighted; all should be the subject of closer analytic study.

The first change is the move in the UK to a reduced transfer period for government records. In the new system that is being implemented, records would be placed in the UK National Archives at Kew under a 20-year rule, replacing the long standing 30-year rule, which was once also the standard, pre-ATIA, in Canada.[49]

The second change has taken place in the United States, following on the issuance, early in the Obama Presidency, of Executive Order 13526. This was a significant and ambitious attempt to reframe the handling of records in the US government system, to provide for their automatic declassification after 25 years and their transfer to the National Archives and Records Administration. A narrowly specified range of records, mostly security related, remains outside the ambit of the automatic declassification scheme and subject to special treatment under the Freedom of Information Act (B1, Information Classified to protect national security).[50]

A third change has taken place in Australia, where the access regime with regards to records generated by Australian security and intelligence agencies remains restrictive, but where the Australian government has decided to invest in the commissioning and publication of a range of independent, official histories of key elements of the Australian community, including ASIO (Australian Security Intelligence Organisation) and DSD (Defence Signals Directorate).[51]

All of these efforts are worthy of deeper examination for Canadian purposes. But they all signal responses among our allies to a common problem of achieving greater transparency and accountability for security and intelligence systems through the preservation of government records, their transfer to national archives, and public openness.

9. Ideas for a way forward

A strategy for declassification and release of historic national security and intelligence is in keeping with the Government of Canada's commitments to open government, to democratic accountability, to learning lessons, and to national security transparency.

To move forward on declassification of national security and intelligence records in a systemic way requires a strong public interest rationale and championing by relevant partners in government. There are, of course, many competing demands for delivery of an "Open Government" philosophy and the case has to be strongly made for attention to the historic records problem.

---

[49] UK National Archives 20 year rule

[50] Executive Order 13526

[51] The Official History of the Australian Security Intelligence Organisation (ASIO) was published in three volumes, covering the years 1945-1989. The first volume, The Spy Catchers: The Official; History of ASIO, 1949-1963, was authored by David Horner; the two subsequent volumes were written by John Blaxland; for the ASD official history, see Georgia Hitch, ABC News, Australian Signals Directorate emerges from the shadows to commission history of itself, July 8, 2019

The Office of the Information Commissioner, in keeping with its mandate, has a strong interest in ensuring that the *Access to Information Act* can be an effective instrument of openness, including with respect to sensitive historic records.

The public interest rationale has three branches.

The most important is that public confidence in, and understanding of, the work of the security and intelligence community can be bolstered by a process of opening historic records to allow for a flourishing of research, an expanded public literature, an improved historic memory, and an understanding of the key drivers of continuity and change in national security.

Canada has a rich and important history in the national security arena, much of which remains unknown because of lack of systemic access to archival records. The Canadian literature on national security and intelligence lags seriously behind our main counterparts in the Five Eyes community.

A second component of the argument is that the security and intelligence community itself benefits from the availability of a strong historic memory of its institutions and work. The preservation of institutional memory can aid in recruitment, training, in performance, in learning lessons, and in the maintenance of strong internal cultures.

A third component is that an effective declassification strategy for national security and intelligence records can both assist the investigative function of the OIC, by lowering the burden of resolving a multitude of individual complaints, and can assist federal departments and agencies in devising an efficient records management system.

Declassification of national security and intelligence records poses the following key questions:

How should exemptions to declassification be understood? In particular, how should a harms test be defined, how should discretion be exercised and managed, and how should declining sensitivity of records over time be calculated?

When should NS and I records be declassified? Assuming the need for a universal, mandated standard rather than the current, piecemeal exercise, what kind of time standard should be put in place?

How should NS and I records be declassified? Here there is a need for a stronger, more transparency-focused, balancing of the discretionary harms test applied to exemptions under the ATIA with considerations of public interest and declining sensitivity over time.

Who should be the controlling authority for declassification? The key issue here is whether declassification authority should rest with individual government departments and agencies, or centrally with Library and Archives Canada. An

alternative option would require asking what kinds of partnerships between LAC and federal departments and agencies might be an optimal?

How can maximum public and government benefit be derived from declassification of NS and I records? Should this benefit include investment in official histories for public release and the creation of releasable record sets with accompanying narratives?

Each of the above questions is complex and cumulatively they have stymied past efforts at reform. But practical answers are possible with sufficient will, necessary changes to law and regulations, sufficient resources, and the ever-important and ongoing culture shift rooted in changing mindsets and enhanced training.

In considering how to counter resistance to change and assuage concerns about release of national security and intelligence records, it might be worth noting the brief presented by a former senior public servant, Mel Cappe, to Parliament with respect to Bill C-58. Mr. Cappe, a former Clerk of the Privy Council, put his emphasis on both the need to define a clear public interest rationale for the release of government records, and the requirement to protect those secrets that truly deserve protection. He put it this way:

"My strong recommendation to the committee is to draw a high wall of secrecy around those functions and categories that need to be preserved to protect the public interest and then make all else open and available to the public. However, the latter openness depends mightily on the secrecy of the former information."

This might be taken as a strategic framework for moving forward, as it puts the focus on declassification, transfer, preservation and openness of public records, and a renewed and updated definition of what constitutes secrets.

A strategic approach to declassification could, taking into consideration the discussion points raised in this paper, contain the following elements:

1. As part of the forthcoming full review of the ATIA, stakeholders, including the OIC, should be asked to submit arguments for revision of the classes of exemptions in the ATIA, particularly sections 13, 15 and 21.
2. As part of the full review of the ATIA, stakeholders, including the OIC, should be asked to submit arguments regarding the creation, preservation and transfer of government records to LAC.
3. Discussions should be held with LAC and TBS regarding the feasibility of a new system for the transfer of NS and I records from federal departments and agencies. Consideration might be given to whether national security and intelligence records should be automatically transferred to the possession and control of LAC after a specified time (10-15-20 years)? Should that requirement be enshrined in legislation and not subject, as at present, to individual (non-transparent) memorandum of agreements between LAC and federal departments and agencies? Would an accountability mechanism for exceptions to a transfer protocol need to be instituted?

4. Consideration should be given to whether national security and intelligence records in the possession of and under the control of LAC could be declassified by delegated LAC officials? Should the final authority rest with LAC?
5. Declassification priorities reflecting judgments about historical significance and the public interest could be established by LAC. These priorities could be established in consultation with an independent advisory group of expert historians and others, as is the practice in the United States. The declassification priorities should also be discussed with the OIC in light of OIC experience with complaints involving such classes of records.
6. The OIC should engage in discussions with Public Safety on linking the National Security Transparency Commitment to proactive release of historic records under NSTC Principle Two.
7. The OIC should engage, alongside other stakeholders, in discussions with TBS to ensure a revised and enlightened statement in TBS Security Management directives with regard to information management security controls.
8. The OIC should help stimulate a discussion with officials at PCO, including the NSIA, concerning the idea of producing special studies, public records sets and official histories illuminating the evolution of the Canadian security and intelligence system.
9. The OIC should discuss with officials at the OAG the potential value of a systems-wide audit of the ATIA regime as a contribution to the full review of the ATIA.
10. The OIC should consider producing an analytic study of the nature of complaints related to national security and intelligence records since 2001, and their resolution, such study to include trend-line analysis. This study could make an important contribution to the upcoming full review of the ATIA
11. The OIC should consider convening an informal advisory group of stakeholders with experience of ATIA and national security records to discuss a declassification strategy in the broad context of potential ATIA reform.
12. The federal government should commission and publish an analytic study of current best practices for the declassification and release of national security and intelligence records, including through sister Freedom of Information Act processes, focused on our Five Eyes partners.
13. The OIC should encourage the Treasury Board Secretariat to include a commitment to the declassification of significant historical records on national security and intelligence in the next iteration of the Open Government Action Plan.
14. The OIC should continue to champion, in combination with the Treasury Board Secretariat, the inclusion of discussions on declassification and public access to historic intelligence and security records as part of the OGP annual summit conference.
15. The OIC, in cooperation with other stakeholders, should encourage the government to commit to creating a central portal for the publication of

> significant national security and intelligence records, whether released through proactive disclosure or through completed ATIA requests. The Open Canada search function for completed ATIA requests is a useful, though limited tool. It provides for a search of completed individual requests but when a completed request is identified, then the researcher is required to make an informal request for a copy of the released records, adding to further delay, more burdens on access units, and ultimately perpetuating a system of atomised, individually held, and fractured records. Records released under access must be considered public records.

Ideas such as these, advanced in the public interest, could help assist the forthcoming review of the ATIA, could help the government operationalize its open government and national security transparency commitments, could potentially strengthen the work of the OIC, and could help the OIC engage with stakeholders and the public in the spirit of modernizing the Canadian access regime.

Key sources for this study

(IN ORDER OF REFERENCE IN THE TEXT)

House of Commons, Report of the Standing Committee on Justice and Solicitor General on the Review of the *Access to Information Act* and the *Privacy Act*, March 1987

Government of Canada, Access to Information Review Task Force, Access to Information: Making it Work for Canadians, June 2002. Archived

Bronskill v. Canada (Canadian Heritage), 2011 FC 983 (CanLII), [2013] 2 FCR 563

Office of the Information Commissioner, Special Report to Parliament, Striking the Right Balance for Transparency: Recommendations to Modernize the *Access to Information Act*, March 2015, See especially Chapter 4: Maximizing Disclosure"

Bill C-58, An Act to Amend the *Access to Information Act*…

Library of Parliament Legislative Summary of Bill C-58, publication no. 42-1-C58-E, revised August 1, 2018

Public Safety Canada, National Security Transparency Commitment

Canada's Action Plan on Open Government 2012-2014

Canada's Action Plan on Open Government 2014-2016

End-of-Term Self-Assessment Report on Action Plan on Open Government 2014-2016

Third Biennial Plan to the Open Government Partnership (2016-2018)

End-of-Term Self Assessment Report on Canada's Third Biennial Plan to the Open Government Partnership 2016-2018

Canada's 2018-2020 National Action Plan on Open Government

Information Commissioner of Canada, letter to the Honourable Scott Brison, President of the Treasury Board, September 18, 2018, copy courtesy of the OIC

Treasury Board Secretariat, Directive on Security Management, July 1, 2019

Treasury Board Secretariat, Security Organization and Administrative Standard, rescinded June 28, 2019

Library and Archives of Canada Act

Treasury Board Secretariat, Interim Directive on the Administration of the *Access to Information Act*, May 5, 2016

Letter, Information Commissioner to the Honourable Serge Joyal, Senator, Chair, Standing Senate Committee on Legal and Constitutional Affairs, November 1, 2018, copy courtesy of OIC.

Office of the Information Commissioner of Canada, Failing to Strike the Right Balance for Transparency: Recommendations to Improve Bill C-58…

Mel Cappe letter to the House of Commons Committee on Access, Privacy and Ethics regarding Bill C-58, dated November 1, 2017