Canada's Access to Information Act and the Canadian Security and Intelligence Community

Professor Wesley K. Wark
Department of History
University of Toronto

In recent decades, access to information legislation has swept the western world. The first modern act was introduced in Finland in 1951, but inevitably it was US legislation that provided the beacon for other countries. The US Freedom of Information Act came into being in 1966. In the ensuing decades some 46 countries have adopted various forms of access laws, and the trend continues.

Canada, true to a long tradition of taking its time to muse over US initiatives before following suit, introduced its own Access to Information Act in the early 1980s. After considerable Parliamentary debate, the Access Act became law in July 1983.[1]

The Canadian Access Act was not promulgated with the specific intent of creating greater degrees of openness with regard to the activities of the Canadian security and intelligence community. But it is worth noting that discussion of Access issues and the passage of legislation coincided with the work of a Royal Commission established to investigate illegal operations conducted by the Security Service of the Royal Canadian Mounted Police. The end result of the Royal Commission (known as the McDonald Commission) was the transfer of the security intelligence function to a new civilian agency, the Canadian Security Intelligence Service, created in 1984. So, concerns about the clandestine world of intelligence were very much in the air as the Access legislation came into being.

In the realm of intelligence and security operations, all Access acts confront a problem and a dilemma—the problem is secrecy; the dilemma is how to peel back such secrecy in a responsible and effective manner.

Perhaps one way to understand this problem graphically is to recall the security stamp that was emblazoned on all historic (or as the British refer to them "aged") records that were of special sensitivity and code-word protected. The stamp read "NEVER TO BE SEEN BY UNAUTHORIZED EYES." This was not a uniquely made-in-Canada stamp. It was part of a system devised to protect intelligence records, first introduced during the Second World War and subsequently extended into the Cold War era. The system was applied to Canadian, British and U.S. records as one of the many developments that occurred in the evolution of the North Atlantic intelligence alliance.

To give security officers the benefit of the doubt, it is probably the case that they meant the weight of the injunction to rest on unauthorized eyes, rather than stressing the eternality of secrecy. But in Canada, and indeed in all democratic jurisdictions, we still face the problem of "NEVER TO BE SEEN…"

Any discussion of the effectiveness of Access laws in dealing with the problem of secrecy of intelligence records will be obscured unless two essential, and I hope obvious, points are established.

The first is that governments in general, and the Canadian government in the case of this discussion, have secrets to protect. Some of these secrets are generated by their own security and intelligence communities in the course of collecting, assessing and disseminating intelligence reports; some of these secrets are matters of internal security, with heightened concerns these days for issues of critical infrastructure protection. Some of the secrets that must be protected are generated by foreign governments and organizations and come into Canadian hands through bilateral and multilateral intelligence sharing arrangements. In the Canadian case, membership in the so-called Quadrapartite Pact, which links the security and intelligence communities of Canada, Britain, the United States and Australia, puts a special onus on Canada to protect both its own and allied-generated intelligence information. Membership in this pact, which in embryonic form dates back to the Second World War, is regarded as vital to Canadian interests. Security lapses, or a perception of security weakness would potential cause grave damage to Canada's reputation and membership.

The second general point that must be established is that security and intelligence communities benefit in many ways from public knowledge about their activities. An informed public is crucial to the democratic acceptability and effective performance of security and intelligence operations. The absence of a reasonable degree of public knowledge of intelligence threatens, among other things, quality recruitment into the agencies concerned, public support, political understanding (especially vital in the senior ranks of the civil service and among political decision-makers), and the very stature of intelligence work. Without an information regime in which citizens have access to knowledge about security and intelligence, popular culture mythology will flourish and fill the vacuum. Nothing could be more harmful than a public understanding of intelligence shaped solely by images of James Bond, George Smiley, and the conspiracy stories so favoured by Hollywood.[2]

The obvious conclusion to draw from these two points is that states require a carefully crafted system to balance competing requirements. Such a system has to balance the legitimate need to protect security with the equally legitimate need to provide public access to the raw materials of knowledge, which are the records generated by agencies of the security and intelligence community.

The right kind of information regime is not easy to build. It depends fundamentally on finding the right answer to the question of balance, which is itself a matter of expectations. So, what kind of balance should we expect in Access legislation?

My view is that the most reasonable expectation upon which to build Access laws and practises is to anticipate a liberal access to historic records, and a highly restricted access to contemporary records. The key distinction here is, of course, the age of the record. The passage of time dilutes the sensitivity of intelligence records. Threats change, countries come and go, technology advances. There are no "eternal" secrets, and the notion that there is some class of records that deserve "NEVER TO BE SEEN" is ludicrous.

While it is reasonable to expect only highly restricted access to contemporary records, this is not to argue that the security and intelligence community should be allowed to clam up entirely. Intelligence agencies are wedded to secrecy and live within a culture of secrets. They need to learn to differentiate between necessary secrets and the value of openness. But we have to face the fact that the determination of the sensitivity of contemporary classified records dealing with such matters as operations, policies and assessments, have to be left to the agencies that control such records. We have to rely on the existence or nurturing of a culture within the intelligence community that recognizes the value of public knowledge and acts accordingly, being as proactive as possible about openness and access to records. This is in the best interests of the community and they should see themselves as having a duty both to inform the public and even to battle the mythologies generated by popular culture.

To understand the balance required between secrecy and openness we need to see Access laws as an implicit bargain. Security and intelligence agencies are given the necessary powers to control contemporary records. In return, there is a recognition that the public should have broad access to historic records, ones that have passed out of the umbra of sensitivity.

This bargain does not describe the current reality in Canada. In looking in more detail at the Canadian case, we may come to understand more fully some of the pitfalls that can emerge in even the best-conceived systems.

The Canadian Access to Information Act proclaims a general right of citizen access to government records.[3] It balances that right against a recognition of the need to protect secrets, by providing for a range of exemptions. These exemptions protect certain kinds of government controlled records from public release. Section 13 of the Act exempts records obtained in confidence from foreign governments and entities. Section 15 of the Act exempts sensitive records dealing with issues of diplomacy, military operations and national security. These two sections of the Act are those most widely cited to block the release of records dealing with security and intelligence issues.[4]

On the face of it, the Canadian Act finds a reasonable balance. But how does it work in practice? The Act has come under recent scrutiny by a government Task Force that issued a report to the Treasury Board, which is responsible for the administration of the Act. The Task Force was put to work because of widespread concerns about the machinery of the Act, inadequate resources, and long delays in acting on Access requests. It was established in August 2000 and delivered its report in June 2002. The report is a public document and is available on the Task Force's web site at

www.atirtf-geai.gc.ca

The report is worth studying, not least because it was a mighty endeavour which produced, to my mind at least, a disappointing mouse. Although the report is disappointing for those who were arguing for reforms to the Access Act, it does contain some illuminating surprises.

One surprise concerns who uses the Access Act. Statistics collected by the Task Force indicated that the leading user by far was a societal group not precisely defined but simply labelled "business." This category of users accounted for fully 40 percent of all requests. Parliamentarians, by the way, accounted for a respectable 10 percent of users of the Act.[5]

The statistics also make clear who does not use the Act. A societal group, also vaguely defined, as "academics" (which I take to comprise private scholars, University professors and graduate students doing research) accounted for only 0.8 percent of the total.[6]

These figures show not just who uses the Access Act in Canada, but who the Act is for, and who it is not for. Consciously or unconsciously, the Canadian Access to Information Act was designed using a business metaphor. Government archives are regarded as a marketplace; citizens are regarded as consumers. Records are like shiny apples. In keeping with this business metaphor, the assumption on which the system is based is that consumers wanted to pick individual shiny apples for their private enjoyment. The only odd thing was that the Access Act does not really charge the consumer (fees are minimal), it just makes it difficult, time-consuming, and cumbersome to get that apple of the consumer's eye.

What is wrong with applying such a business metaphor? The fundamental problem is that government records are not a marketplace, not a grocery store. A document archive, as any researcher, librarian, or record keeper will tell you, consists of carefully interwoven strands of information, usually arranged in departmental files on a chronological and/or subject basis. Altogether such records comprise an organic whole. They cannot be treated or understood in atomised fashion, as individual pieces of paper. Yet this is how the Access act

renders such records. It leaves the opening of government records to individual consumers, and it results in the fragmentation of records that can only be fully understood if their coherence and original organization is retained. The system might just work in a state where massive scholarly and private sector resources can be applied to records requests—as in the United States.[7] It cannot function successfully in a state such as Canada where such resources do not exist.

In application, the Canadian Access Act has been no less than a disaster. But I can only hope that it is an illuminating disaster from which others can learn lessons.

There are two essential reasons for the failure of the Canadian Access Act. One was, I think, an unintended consequence of the Act. When the Access Act was proclaimed, and especially once requests began to mount, finite government resources in records management inevitably shifted to a focus on handling Access issues. This had the effect of bringing to a standstill any real programme for the systematic release in bulk of historic records. The original Access Act had stipulated that it wasn't the intention of the government to rely on its mechanisms alone to ensure orderly release to the public of government information. But resource constraints imposed hard choices and Access became the first priority. The recent Access Task Force Review again stipulated that the government should find ways of releasing information outside the confines of the Act, but in the absence of new resources and a new culture in government, it is hard to see how this wish will turn into reality.[8]

More fundamental still, the Access Act overlooked the problem of "NEVER." It failed to institute any requirement to release records en masse and in coherent fashion after the passage of a specified period of time. Prior to the Access Act, Canadian records release had been governed, following the British model, by a thirty year rule. With the passage of the Act, the thirty year rule was abandoned and no specific time horizon was placed on public access to records. The drafters of the original Access Act were warned by, among others, the Canadian Historical Association, about the need for a time horizon for documents release, but this advice was ignored. The Access Task Fork was warned again about the need to reinstate something like a thirty year rule. This advice was ignored again, on grounds that I think are spurious.

The relevant section of the Review reads as follows:

"The Task Force agrees that records should not be 'eternally exempted' from disclosure and that a mechanism is needed to trigger the release of records that are no longer sensitive. In examining this issue, however, we concluded that a rule requiring the automatic release of government records after any specific time period would not yield the desired results. For example, some exemptions include criteria for assessing probable harm, which should enable records to be released well before the 30 years is up. In such cases [which, it has to be noted,

are hypothetical], the insertion of a 30-year rule in the Act might well result in later release than is now the case."[9]

The Task Force goes on to comment:

"As well, certain other exemptions are designed to protect information that can be sensitive for a much longer period of time. In these situations, the release of the information could still harm national interests or individuals, even after 30 years."

In other words, we are still in the land of "NEVER."

The only solution that the Task Force Review advances is the weak one of turning this intractable problem over to the National Archives and encouraging it to play a lead role in "developing and adopting processes for the systematic bulk review and release of historic records."[10] But such systems already exist for records deemed non-sensitive. For sensitive records, archivists themselves are quick to note that it is not their job to force open government archives. Instead what matters to national archivists is their carefully nurtured relationship with government departments. This relationship is the foundation on which they must work to ensure adequate record keeping and management and the orderly transfer of materials from originating agencies into the safekeeping of the Archives itself. Archivists must play the game of document diplomacy. Anything that would introduce tension and mistrust between the National Archives and government departments threatens what they regard as their single most important mandate—the preservation and long term safe-keeping of records. Nothing would be more calculated to sour relations between the National Archives and government than efforts on the part of the Archives to take the lead in forcing open classes of sensitive records.

The Access to Information Review Task Force report leaves the situation with regard to Canadian security and intelligence records essentially unchanged. The government has strong tools in the Access Act to prevent the release of sensitive, contemporary records. There is no incentive and no system to provide for the release in organized fashion of historic records.

The end result of the Canadian Access Act has been to stifle public knowledge of security and intelligence issues. Against all logic, the Access Act has resulted in non access. For researchers who wish to study the activities of Canadian security and intelligence agencies, the only fruitful area concerns World War Two. The availability of open records, combined with voluntary transfers of some key intelligence records, specially regarding signals intelligence, makes for a potentially critical mass of material. The only drawback is that the Second World War period is one in which Canadian security and intelligence was still in its infancy—there are interesting experiments and innovations, but the work remained embryonic.

The more critical period for the development of the Canadian intelligence community was, of course, the Cold War. But thanks to the Access regime and the removal of the thirty year rule, there are insufficient records available to research this era in any depth. Recourse to the Access Act to pry open records is like playing roulette. You can't guess the outcome and extraordinary levels of patience are required. For most "academics," the game is not worth the candle. The Access Act functions, in effect, as a deterrent. This explains the startling figure cited by the Review Task Force—that only 0.8% percent of Access users are "academics."

The costs of ignorance with regard to security and intelligence functions have already been alluded to. On-going secrecy and the absence of a well founded knowledge of the intelligence function not only upset the implicit bargain on which the right to secrecy operates, but threaten the legitimacy and effectiveness of security and intelligence agencies themselves.

Something needs to be done to break the impasse. Despite the findings of the Review Task Force, changes are urgently needed to the Access Act. But immediate redress in terms of the Access Act is unlikely. The failure of the Review has undermined any such process for the near future, at least.

Alternative hopes rest with the enlightened self-interest of the intelligence community. Security and intelligence agencies need public recognition and public support. They, not the National Archives, should take the lead and be genuinely proactive with regard to records release. There are a number of ways in which this could be done:

1. The intelligence community should be encouraged to create a historical office as a focal point for records management, overview of records keeping, international liaison on records issues, policy advice, and even post-mortem studies. The US Central Intelligence Agency has had success with such an approach since the establishment of their "Center for the Study of History."

2. The intelligence community should identify, with the help of an advisory panel of outside experts, key classes of post-1945 records. These records should be subjected to bulk review and strategically released, starting with such central material as the papers of the Joint Intelligence Committee and its sister body, the Communications Research Committee. The release could follow an informal thirty year rule.

3. The intelligence community must work to modernize its own culture of secrecy, especially by instituting a critical sense of the value of historical knowledge and by educating its own officials in the declining sensitivity of secrets over time.

Unfortunately, the events of September 11, 2001 and its aftermath have had a spill-over effect on Canadian official attitudes towards secrecy. Some of this effect is natural and warranted, especially in regard to a concern about tightening the controls over current operational information and over information relating to critical infrastructure security. The Canadian government introduced an omnibus Counter-Terrorism bill (C-36) in October 2001. After much public debate it was passed into law in December. Among the many items that found their way into this omnibus legislation was a little-noted alteration to the Official Secrets Act, renamed the Security of Information Act. The revised Act created a class of intelligence officials who were to be deemed, on the basis of their handling of sensitive information, "persons permanently bound to secrecy." There were no time limits placed on the reach of this proviso, nor any suggestion of appeal or adjudication. Taken in a literal sense, the clause would make illegal and subject to stiff penalty any effort on the part of even long-retired intelligence veterans to discuss the nature of their work, or to publish their memoirs. It was another reiteration of the antique philosophy of "NEVER TO BE SEEN BY UNAUTHORIZED EYES."

There are two final, and perhaps gloomy, points to make. Even the best Access system in the world is going to be of little value if there are, in future, no records to access. We are living in the midst of an information and communications revolution, which is having a profound effect on the maintenance of paper, or Gutenberg-era, records. Intelligence communities, in particular, are growing ever more dependent on electronic information storage and communication, especially via e-mail. The transience of e-mail messages is well known and current information management systems have no real solution to the e-mail problem, nor to the problem of the long-term viability and readability of computer generated data.

The second baleful reflection is that Access laws can have unintended consequences. One that is worrisome in the security and intelligence arena, is that the existence of concerns about the security of records, can lead intelligence officials to shun careful record keeping and to be wary of committing certain kinds of messages and thoughts to paper, or its electronic equivalent. Again, we must not end up in a world in which Access laws leave us nothing to access.

The key to change is that we must find a way, via access regimes and changes to the culture of secrecy, to replace dated Cold-War era injunctions of "NEVER TO BE SEEN BY UNAUTHORIZED EYES" with the more enlightened and sensible "EVENTUALLY TO BE SEEN BY UNAUTHORIZED EYES."

NOTES

[1] A brief summary of the origins of the Canadian Act can be found in Government of Canada, Access to Information Review Task Force, Report, "Access to Information: Making it Work for Canadians, June 2002, Annex 8. The Report, hereafter cited as Access Report, is available on the web at www.atirtf-geai.gc.ca

[2] A recent example of Hollywood's fascination with intelligence and conspiracy, which can perhaps be traced back to the film, "The Manchurian Candidate," is "Enemy of the State." Released in 1999, the film features an elaborate plot by a conspiratorial group within the National Security Agency to assassinate a Congressman who opposes a new surveillance bill.

[3] Access To Information Act, R.S. 1985, c. A1, s. 1

[4] For a taste of the broader debate on Canadian Access laws and practises, see the work of Alasdair Roberts, including his recent "New Strategies for the Enforcement of the Access to Information Act, Queen's Law Journal, 27, Winter 2002. Underlying social change is explored in Neil Nevitte, The Decline of Deference: Canadian Value Change in Comparative Perspective (Toronto: Broadview Press, 1996)

[5] Access Report, Introduction, p. 9

[6] Access Report, Introduction, p. 9

[7] Among US private sector organisations that work to ensure access to intelligence and security records is the National Security Archive. Their annual report is posted at www.nsarchive.org (July 2001)

[8] Access Report, Chapter 8, p. 139

[9] Access Report, Chapter 8, p. 138

[10] Access Report, Chapter 8, p. 139