Dalhousie Journal of Legal Studies

Volume 24 Article 1

1-1-2015

Edward Snowden: Hero or Traitor? Considering the Implications for Canadian National Security and Whistleblower Law

Mark Friedman

EDWARD SNOWDEN: HERO OR TRAITOR? CONSIDERING THE IMPLICATIONS FOR CANADIAN NATIONAL SECURITY AND WHISTLEBLOWER LAW

Mark Friedman*

ABSTRACT

Edward Snowden's disclosures of secret National Security Agency documents have significant implications for Canadian national security law. Snowden's revelation that the Communications Security Establishment Canada (CSEC) attempted to spy on the Brazilian government is analyzed to determine: first, whether economic intelligence gathering is a legal function of CSEC; and, second, whether CSEC employees would be afforded protection by the *Security of Information Act* (*SOIA*) if they decided to reveal the existence of such a program. Since whistleblower protection for intelligence agency personnel has never been tested in Canadian courts, the author draws on different areas of law to fill a void in Canadian legal literature and jurisprudence. In this respect, Snowden's case allows observers to imagine how whistleblower protection might operate and, in doing so, provides a case study to determine whether *SOIA*'s provisions are overly restrictive or lenient. Ultimately, the author suggests that CSEC's statutory framework permits the organization to spy on a foreign government for economic intelligence. Furthermore, whistleblower protection law would not protect Snowden because the manner in which he disclosed secret information does not comply with the framework set out in the *SOIA*.

Citation: (2015) 24 Dal J Leg Stud 1.

* Mark Friedman received his J.D. from Osgoode Hall Law School. He holds an M.Sc. in Theory and History of International Relations from the London School of Economics and a B.Soc.Sc. from the University of Ottawa. The author would like to thank Professor Ron Atkey and Edward Murphy for reviewing earlier drafts of this article.

INTRODUCTION

Hero. Traitor. Whistleblower. Leaker. "Grandiose narcissist who deserves to be in prison."[1] In what has been described as the "the most serious compromise of classified information in the history of the US intelligence community,"[2] Edward Snowden's disclosure of National Security Agency (NSA) intelligence documents has unlocked wider debates concerning the perceived surrender of privacy rights for national security interests. The impact of these leaks is not limited to the United States (US). The story is of particular interest for Canada because among the documents that Snowden uncovered was a slideshow that revealed the Communications Security Establishment Canada (CSEC) had engaged in economic espionage against Brazil's Ministry of Mines and Energy. This was the first of several Snowden leaks concerning CSEC activity and raises important questions regarding the utility and legality of spying on countries with which Canada enjoys amicable economic and diplomatic ties.

The purpose of this article is two-fold: first, to consider the legality of the espionage program; and second, to examine whether Snowden's decision to expose the program would have been legal if he were an employee of the Canadian government and subject to Canadian secrecy laws. Is Snowden a hero for making Canadians aware of CSEC's activities, and would a Canadian court reach the same conclusion? This is the focus of the hypothetical case study.

In Part I, the article will outline the legislative parameters guiding CSEC, a close-knit agency of approximately 2,100 employees with a rising annual budget that stood at over $460.9 million when the slideshow was leaked in 2013.[3] Next, the legality of CSEC's alleged operations in gathering economic intelligence in Brazil will be examined; the outcome of this analysis will directly affect a

---

1 Jeffrey Toobin, "Edward Snowden is No Hero", *The New Yorker* (10 June 2013), online: <www.newyorker.com/news/daily-comment/edward-snowden-is-no-hero>.

2 "Edward Snowden's leaks most serious in US history: ex-CIA official", *NDTV* (26 October 2013), online: <www.ndtv.com/world-news/edward-snowdens-leaks-most-serious-in-us-history-ex-cia-official-538988>.

3 This is over 4.5 times larger than CSEC's budget in 1999. The fact that the government has earmarked over $1.2 billion to construct a new building for the agency also underscores the expanding role and prioritization of the agency within Canada's wider security apparatus. See Colin Freeze, "How CSEC became an electronic spying giant", *The Globe and Mail* (30 November 2013), online: <www.theglobeandmail.com/news/politics/how-csec-became-an-electronic-spying-giant/article15699694> [Freeze, "How CSEC became"].

determination of whether Snowden's disclosure of the program was itself legal. In Part II, the article will briefly discuss the history of unauthorized disclosures in the US, and how this history informs the extensive use of the *Espionage Act* to clamp down on 'leakers' today. This situation will be contrasted with Canada's experience under the *Security of Information Act*. In Part III, the paper will discuss Canadian laws that govern whistleblower protection for civil servants in the intelligence community and compare those laws with American legislation. Lastly, it will put Snowden on trial; if Snowden were charged for publicly releasing secret information about Brazil, would he have a workable defence under Canada's whistleblower protection laws?

In undertaking this analysis, this article suggests that CSEC's broad mandate to collect foreign intelligence includes the gathering of economic intelligence from foreign ministries. With regard to whistleblower protection, the paper determines that Snowden would not have a defence in Canada to justify his public disclosures, despite the greater protection afforded to whistleblowers in Canada than in the US.

I. CSEC AND THE LEGALITY OF ECONOMIC ESPIONAGE

On October 6, 2013, the Brazilian television network *Globo* extracted a CSEC-created slideshow from the trove of Snowden's information treasury.[4] The slideshow, a June 2012 CSEC presentation before the NSA, discussed the former's plans to spy on the Brazilian Ministry of Mines and Energy through a program called Olympia. The content of the slideshow suggests that CSEC sought to monitor Brazilian e-mail and telecommunications in order to gather economic intelligence. The plan and its publication in the media placed the discreet organization front and centre in international headlines.

CSEC's ex-chief, John Forster, defended the organization, saying "everything that CSEC does in terms of foreign intelligence follows Canadian

---

4 "Canadian spies targeted Brazil's mines ministry: report", *CBC News* (7 October 2013), online: Canadian Broadcasting Corporation <www.cbc.ca/news/canadian-spies-targeted-brazil-s-mines-ministry-report-1.1927975>.

law."[5] However, that did not stop the organization from being criticized in public media. The slideshow suggested that CSEC had become unruly and unconcerned with the diplomatic consequences of or legal constraints on its actions.[6] A particularly concerning aspect of CSEC's spying was that the information it gathered from Brazil could be forwarded to Canadian corporations seeking to weigh the viability of investment opportunities. Effectively, the Canadian government proposed to spy on behalf of private interests instead of working exclusively for the 1,000 government departments and agencies for which CSEC provides information.[7]

Collecting economic intelligence is not new to CSEC. For instance, CSEC spied on envoys from Mexico and Uruguay during respective multilateral trade negotiations in the 1980s and 1990s.[8] The difference now is that the *National Defence Act* (*NDA*)[9] restrains CSEC's activities. As University of Ottawa Professor Craig Forcese notes, CSEC must act in accordance with its mandate when intercepting foreign intelligence. Thus, the only way CSEC's economic intelligence gathering could be lawful is if its actions fit within the organization's statutory mandate.[10]

Under section 273.64 of the *NDA*, CSEC is responsible for acquiring and using information derived from the "global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities." While the mandate is broad, the *NDA*'s definition of key terms narrows the scope of CSEC's legal parameters. Under section 273.62, foreign intelligence is defined as "information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or

---

5 "More Intelligence, Please, About Intelligence", *The Globe and Mail* (14 October 2013), online: <www.theglobeandmail.com/globe-debate/editorials/more-intelligence-please-about-intelligence/article14847584> ["More Intelligence"].

6 *Ibid.*

7 Freeze, "How CSEC became", *supra* note 3.

8 Martin Rudner, "Canada's Communications Security Establishment: from Cold War to Globalisation" Occasional Paper No 22 (Carleton University: Norman Patterson School of International Affairs, 2000) at 28.

9 *National Defence Act,* RSC 1985, c N-5, s 273.66 [*NDA*].

10 Since the foreign intelligence collected from Brazil did not have a Canadian nexus, there are no other statutory rules that would circumscribe CSEC's activity. Ministerial authorization is only required for interceptions that involve a Canadian or a person in Canada. See Craig Forcese, *National Security Law: Canadian Practice in International Perspective* (Toronto: Irwin Law, 2008) at 455; *NDA*, *supra* note 9, s 273.65.

terrorist group, as they relate to international affairs, defence or security." Therefore, unless there is a clear nexus between the intelligence gathered and international affairs, defence, or security, CSEC is not authorized to gather it.

While the *NDA* does not provide definitions of international affairs, national security, or national defence, an overview of court decisions in other areas of law may be useful to determine their scope. In *Canada (Attorney General) v Almalki*, a 2010 decision of the Federal Court, Justice Mosley reviewed the government's ability to withhold information under the *Canada Evidence Act* for the sake of "national security, national defence, or international relations."[11] The Court found that national defence should be defined as "all measures taken by a nation to protect itself against its enemies." Meanwhile, Mosley J. interpreted national security as "the preservation of the Canadian way of life including the safeguarding of the security of persons, institutions and freedoms in Canada."[12]

The Canadian government would not be able to substantiate the Olympia operation on defence or security grounds if these definitions were applied to CSEC's mandate. For one, CSEC could not ground Olympia as a defence matter because Brazil is a non-enemy country with which Canada has a friendly diplomatic relationship. Nor could CSEC demonstrate that its activities were security-related, unless it was able to somehow prove that Brazilian energy companies threatened the livelihoods and liberties of Canadians.

The only other possible legal justification for CSEC's activities would be that this collection of foreign intelligence pertained to international affairs. As noted above, the term "international affairs" is undefined in the *NDA*; however, the phrase also appears in the *Access to Information Act*. In summarizing the current state of the law, the Office of the Information Commissioner borrowed from Oxford Dictionary definitions to define "international affairs" in two parts: international, as in "existing, involving, or carried on between two or more nations"; and affairs, as in "a concern; a business; a matter to be attended to…"[13]

---

[11] *Canada (AG) v Almalki*, 2010 FC 1106, 333 DLR (4th) 506 [*Almalki*].

[12] *Ibid* at paras 77–8.

[13] Office of the Information Commissioner of Canada, "Section 15: International Affairs and Defence", online: <www.oic-ci.gc.ca/eng/inv_inv-gui-ati_gui-inv-ati_section_15.aspx>. While the Commission noted "it is not possible to define the parameters/describe the scope of the provision," it provided

If this broad definition of "international affairs" is applied to the *NDA*, then CSEC's spying in Brazil would fall within the scope of its mandate. As a potential competitor to Canadian industry and interests, the activities of the Brazilian Ministry could be reasonably construed as a subject of international "concern" or a "matter to be attended to."

While the decision to take a liberal interpretation of "international affairs" has a legitimate legal basis, such a reading has serious and far-reaching implications. As the *Globe and Mail*'s editorial board argues, under this definition international affairs "could cover the activities of the most innocent non-Canadian NGO and the most humdrum, law-abiding, non-Canadian business that operates in more than one country."[14] The ability to gather such expansive foreign intelligence under the guise of "international affairs" suggests the need for a more refined approach. While the current *NDA* does not specify the purposes of CSEC's powers or mandate, revisiting the legislation that first codified CSEC—the *Anti-terrorism Act*—is helpful to delineate the organization's *raison d'etre*. The *Act*'s preamble emphasizes, among other things, the need to combat terrorism and to maintain international peace and security.[15] Refocusing the notion of foreign intelligence to specifically address these objectives may help crystalize the meaning of "international affairs." Otherwise, the status quo effectively maintains CSEC's ability to pursue economic espionage under the cloak of broadly worded, imprecise legislation.

II. THE *ESPIONAGE ACT* AND *SECURITY OF INFORMATION ACT*

In Canada, as in the US, it is illegal for an intelligence officer to divulge secret information. However, this restriction is subject to whistleblower protection measures.[16] Before turning to Snowden, it is worth examining the legal

examples of information that *may* fall under the ambit of international affairs. The examples focused predominantly on inter-state diplomatic relations; however, the Commission also listed "information relating to sensitive matters (for example, Canadian sovereignty in the Arctic) for the country" as information that may fall under the category. While the examples are merely illustrative, it is possible that the spying program could be construed as a "sensitive matter for the country" as well.

[14] "More Intelligence", *supra* note 5.

[15] *Anti-terrorism Act*, SC 2001, c 41.

[16] *Security of Information Act*, RSC 1985, c O-5, ss 13–14 [*SOIA*].

mechanisms used in both jurisdictions to prohibit disclosures of secret information, including disclosures such as the CSEC slideshow, which was classified as "Top Secret."[17] By analyzing the American legislation under which Snowden has actually been charged, it will be easier to assess how and whether he would be charged if he had disclosed the same information as a Canadian intelligence worker. In this respect, Snowden's now infamous revelations offer analysts a useful case study to test how Canadian secrecy and whistleblower protection laws might operate.

The *Espionage Act* in the United States

The US *Espionage Act,* originally passed during the Red Scare in 1917, is most commonly understood as prohibiting persons sworn to secrecy from delivering classified information to foreign governments. This type of "classic spying" is well known from the cases of Julius and Ethel Rosenberg and Robert Hanssen, who were famously convicted under the *Espionage Act* in 1951 and 2002, respectively. However, the *Espionage Act* also criminalizes any disclosure of information relating to national defence, irrespective of whether the responsible party was a member of a foreign government. American jurisprudence defines the meaning of "information relating to national defence" broadly. It includes any information closely held by the government that, if disclosed, could harm the US,[18] which would seem to include information concerning international affairs. Snowden has been charged under section 793(d) of the *Espionage Act,* which reads:

> (d) Whoever, lawfully having possession of, access to, control over, or being entrusted with any document…relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates…or attempts to communicate… the same to any person not entitled to receive it;
>
> […]

---

[17] Colin Freeze, "Read a CSEC document that was first acquired by Snowden", *The Globe and Mail* (30 November 2013), online: <www.theglobeandmail.com/news/politics/read-a-csec-document-on-brazil-that-was-first-acquired-by-edward-snowden/article15699941> [Freeze, "Read a CSEC document"].

[18] *United States v Rosen,* Case No 1:05cr225 (ED Va, 9 August 2006) at para 20 [*Rosen*].

> Shall be fined under this title or imprisoned not more than ten years, or both.[19]

Just as "information relating to national defence" has been interpreted expansively, so too has the clause "to any person not entitled to receive it."[20] While the US Supreme Court averred in the 1941 decision *Gorin v US* that violations under the *Espionage Act* require "bad faith" on the part of the person making a disclosure, more recent jurisprudence has taken a broad view of what "bad faith" entails.[21] According to *US v Rosen*, a 2005 decision of the US District Court for the Eastern District of Virginia, bad faith requires the person to have "reason to believe the disclosure could harm the United Sates or aid a foreign government."[22] *Rosen* follows the precedent set by the Fourth Circuit in the 1988 case *US v Morison,* in which the court ruled that the government does not need to demonstrate the defendant *intended* to cause harm.[23] This interpretation of section 793(d) affords more latitude and favour to the state in prosecuting whistleblowers who may have acted with the goal of advancing the public interest.

The liberal interpretation of section 793 has been applied and elaborated in light of the government's shift toward using the *Espionage Act* for targeting 'non-traditional' leakers more vigorously. Six of the nine persons accused or convicted under the *Espionage Act* for releasing information to the press, including Snowden, have been charged or convicted during President Barack Obama's administration.[24] There are three prevailing rationales that explain the US government's recent focus on leaks to the media. First, the 9/11 terrorist attacks intensified the need to prevent non-state actors from gaining access to classified information. In the past, states were predominantly concerned with protecting their information from other foreign states. This narrower focus was significantly more manageable for the relevant government agencies. Second, 'leakers' are

---

[19] *Espionage Act,* 18 USC § 793(d). Snowden has also been charged under § 641 and §798(a)(3).

[20] Stephen Vladeck, "The Espionage Act and National Whistleblowing after *Garcetti*" (2008) 57:5 Am U L Rev 1531 at 1537.

[21] David McCraw & Stephen Gikow, "The End to an Unspoken Bargain? National Security and Leaks in a Post-Pentagon Papers World" (2013) 48 Harv CR-CLL Rev 473 at 496.

[22] *Rosen*, *supra* note 18 at para 63.

[23] McCraw & Gikow, *supra* note 21 at 497.

[24] Peter Finn & Sari Horwitz, "US charges Snowden with espionage", *The Washington Post* (21 June 2013), online: *Washington Post* <www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html>.

increasingly emerging from lower levels of government where they are more difficult to supervise. Previously, high-level decision makers would frequently leak information to the press when it suited the administration's interests and when they were able to control the content of the disclosure.[25] However, recent cases against Shamai Leibowitz and Jeffrey Sterling demonstrate that the government is no longer "the only ship that leaks from the top."[26] Related to this point is a third explanation for the government's recent focus on leaks to the media—that is, the digitization of government documents and the relative ease with which massive quantities of information may now be disseminated through the Internet. Case in point: in 2010 Chelsea Manning, a low-level military officer, delivered over 250,000 diplomatic cables to WikiLeaks, a rogue online media entity.[27] The use of novel tools for prosecution, such as section 793(d), signifies both the US government's concern for unauthorized disclosures, as well as the utility of the *Espionage Act* in punishing and possibly deterring prospective leakers.

The *Security of Information Act* in Canada

Canadian secrecy law was originally set out in the 1939 *Official Secrets Act* (*OSA*), which was modelled on the British statute of the same name.[28] As American commentators note, the British *Official Secrets Act* was far more prohibitive than its American equivalent; it criminalized the reproduction of government information by the media and created a reverse onus on the accused to demonstrate that the conduct was not damaging to the state. Professor David Pozen, who specializes in national security and information law at Columbia Law School, observed that "many have asserted that such a law would not be tolerated" in the US.[29] The criticisms levelled against the British legislation were also directed against its Canadian counterpart. The 1969 Royal Commission on

---

[25] David Pozen, "The Leaky Leviathan: Why the Government Condemns and Condones Unlawful Disclosures of Information" (2013) 127 Harv L Rev 512 at 528–9, 592–5.

[26] Mary-Rose Papandrea, "The Publication of National Security Information in the Digital Age" (2011) 5:1 J National Security L & Pol'y 119 at 121.

[27] David Leigh, "How 250,000 US embassy cables were leaked", *The Guardian* (28 November 2010), online: *Guardian News & Media* <www.theguardian.com/world/2010/nov/28/how-us-embassy-cables-leaked>.

[28] Forcese, *supra* note 10 at 422.

[29] Pozen, *supra* note 25 at 626.

Security (sometimes referred to as the Mackenzie Commission) whose mandate was to review government security procedures concluded that the *OSA* was over-inclusive. In 1979, the Ontario Superior Court went so far as to recommend a complete redrafting of the legislation.[30] The statute had also been criticized in the early *Charter* era. For instance, the Canadian Law Reform Commission argued in 1986 that the reverse onus test violated section 11(d) of the *Charter*.[31]

Despite these criticisms, it was not until the Chrétien government passed the *Anti-terrorism Act* (*ATA*) in 2001 that the calls for reform were heeded. As part of the *ATA*, the *Security of Information Act* (*SOIA*) was designed to adequately protect the security interests of the state while respecting due process rights of the accused.[32] To date, the *SOIA* has never been used to charge a person who disclosed information to the press. The only person sentenced under the statute, Jeffrey Paul Delisle, was convicted in 2013 for divulging information to another state.[33]

Under section 14 of the *SOIA,* a person permanently bound to secrecy who intentionally and without authority communicates or confirms "special operational information" is guilty of an indictable offence. Thus, in determining whether Snowden would be subject to the *Act*, a judge would have to first determine whether Snowden was a person permanently bound by secrecy, and then consider whether the information he communicated was "special operational information."

Meanwhile, section 8(1) of the *SOIA* defines a person permanently bound to secrecy as someone who is "a current or former member or employee of a department, division, branch or office of the federal public administration, or any

---

30 Forcese, *supra* note 10 at 422.

31 *Ibid.*

32 Despite amendments to the existing regime, some of the language of the 1939 Act remained intact. For instance, section 4 prohibits the communication of secret information to any person not entitled to receive it. The fact that the provision applies to any person in possession of government information, be it a non-secret civil servant or a journalist, has been ruled unconstitutional for its vagueness and overbreadth, as well as its infringement on freedom of the press. See *O'Neill v Canada (AG)*, [2006] OJ No 4189 (QL) at paras 62, 71, 272 DLR (4th) 193.

33 Since Jeffrey Paul Delisle's conviction, Qing Quentin Huang has been charged under the *SOIA* for providing secret information to the Chinese government. See Stewart Bell, "Ontario's Qing Quentin Huang, accused of spying for China, was 'against capitalism,' former employer says", *National Post* (3 December 2013), online: *National Post* <news.nationalpost.com/news/canada/ontarios-qing-quentin-huang-accused-of-spying-for-china-was-against-capitalism-former-employer-says>.

of its parts, set out in the schedule," which lists CSEC among other national security-oriented government departments and agencies. Although Snowden was a contractor working for the NSA and was not, strictly speaking, a government employee, he would still fall within the scope of the *Act*. CSEC, unlike the NSA, does not employ contractors to fulfill its mandate; however, the scope of persons "permanently bound by secrecy" contemplates the use of contractors as well. Section 10(1) enables a deputy department head to bind any person to secrecy if the person had, has, or will have access to special operational information and it is in the interest of national security to designate the person.[34] In light of this provision, it is reasonable to presume that a person in Snowden's position, with similar access to secret information, would be conferred this status by the Deputy Minister of Defence. Thus, there is little doubt that Snowden would be a person permanently bound by secrecy under the *SOIA*.

Snowden's disclosures would also satisfy the second threshold in section 14, as the information he revealed would qualify as "special operational information." The meaning of the term, as defined in the *SOIA*, includes a wide scope of information including the "means that the Government of Canada used, uses or intends to use, or is capable of using, to covertly collect or obtain, or to decipher, assess, analyze, process, handle, report, communicate or otherwise deal with information or intelligence."[35] For greater certainty, the legislation states that "information or intelligence *similar in nature* to information or intelligence referred to in the above definition that is in relation to, or received from, a foreign entity or terrorist group" is special operational information.[36] Courts could use this clause, along with the definition preceding it, to take a liberal approach to classifying information as "special operational," just as an expansive definition has been accorded to "defence information" under the US *Espionage Act*.

As someone lawfully bound by secrecy who disclosed intelligence-gathering mechanisms and information relating to a foreign entity to the press, Snowden's activities fall under the purview of section 14. Therefore, the question is how each

---

[34] "Deputy head" is defined for the purpose of subsection 10(1) in *SOIA*, *supra* note 16, s 8(2).

[35] *Ibid*, s 8.

[36] *Ibid*.

respective agency would consider Snowden's disclosures, given that the leaks revealed activity that could have potentially compromised the public's interest in government transparency, the adherence to the rule of law, and the preservation of Canada's economic and diplomatic standing. It is to this question that the article now turns.

III. WHISTLEBLOWER PROTECTION AND DEFENCES IN THE UNITED STATES AND CANADA

American and Canadian Approaches to Whistleblower Protection

In the US, Snowden would not be able to avail himself of any whistleblower protections to defend his disclosures of classified information. This is because American law fails to provide any legal protection for NSA government contractors who, like Snowden, report wrongdoing. This is the case notwithstanding the fact that 70% of the NSA's budgets are spent on private contracts.[37] Even protection for US government employees is inadequate. Government employees can report abuse to their Department's Inspector General, the Inspector General of the Intelligence Community, and eventually to Congress, without fearing reprisal.[38] However, the reporting scheme has been criticized as setting whistleblowers up for failure.[39] Apart from the bureaucratic hurdles that employees would have to overcome, they may also find themselves in the uncomfortable position of reporting to the very people responsible for approving or shielding the questionable activity.[40]

---

[37] RM Perry, *Intelligence whistleblower protections: In brief* (Washington: Congressional Research Service, 2014) at 2, 7; Tim Shorrock, "Meet the Contractors Analyzing your Private Data", *Salon* (10 June 2013), online: <www.salon.com/2013/06/10/digital_blackwater_meet_the_contractors_who_analyze_your_personal_data>.

[38] *Intelligence Authorization Act for Fiscal Year 2014*, PL 113-126, 128 Stat 1390, 1414 (2014). See also Perry, *supra* note 37 at 2–4.

[39] Pozen, *supra* note 25 at 527.

[40] David Axe, "Obama order protects intelligence community whistleblowers" (15 October 2012), online: The Center for Public Integrity <www.publicintegrity.org/2012/10/15/11473/obama-order-protects-intelligence-community-whistleblowers>. On retaliation against whistleblowers, see also Perry, *supra* note 37 at 6.

Most troublingly, there is "absolutely zero protection" for whistleblowers who release information to the media, even when they reveal illegal activity.[41] The inability to report to the media removes an important tool in the arsenal of the whistleblower. Government agencies may wilfully ignore threats to publicize information because they are secure in their knowledge that a person cannot rely on a whistleblower defence when publicly releasing information. The irony, of course, is that only an illegal act from a whistleblower could expose an illegal program. This demonstrates the mismatched priorities of the American government: an administration that refused to prosecute torturers would be eager to imprison the person responsible for disclosing the torture's existence.[42]

While the American approach is ostensibly designed to favour the maintenance of national security, a lesson from the Snowden affair may be that the absence of sufficient protections can encourage whistleblowers to pursue channels outside the law and compromise national security to a greater extent than would have otherwise occurred. Although public interests in disclosure and national security are often viewed as mutually exclusive, they should not be viewed as fitting neatly in watertight compartments. Providing some level of protection should be viewed as a means to discourage wholesale leaks that would have an even greater adverse effect than a smaller leak conducted in accordance with the law.

Flowing from this premise, and in contrast to the American approach, the Canadian *SOIA* envisages a public interest defence that enables a national security employee to publicly release information without facing criminal sanction. Section 15 of the *SOIA* exempts a person sworn to secrecy from conviction if "the person establishes that he or she acted in the public interest."[43] Determining whether Snowden acted in the public interest under Canadian law is speculative given that section 15 has never been argued before a judge and academic commentary rarely speaks to its application. However, this uncertainty is precisely what makes Snowden's case fascinating. It allows lawyers to explore how section

---

41 Pozen, *supra* note 25 at 527.

42 Jesselyn Radak & Kathleen McClellan, "The Criminalization of Whistleblowing" (2011) 2:1 Am U Lab & Employment LF 57 at 73.

43 *SOIA*, *supra* note 16, s 15.

15 might operate and provides a case study to determine whether the *Act*'s provisions are overly restrictive or lenient in comparison to the equivalent American legislation.

A cursory examination indicates that section 15 would not be available as a defence for Snowden. Before CSEC employees can disclose secret material, section 15(5) requires them to first bring their concerns to the attention of the deputy head or the Deputy Attorney General as well as the CSEC Commissioner. By disclosing the NSA's activities directly to a journalist without informing the relevant officials beforehand, Snowden did not follow the procedure under section 15. The more interesting question is whether Snowden would be protected under the public interest defence if he had exhausted the internal processes under section 15(5). In other words, would Snowden be permitted to release the Brazilian slideshow after discovering its existence in the course of his employment, assuming he had already notified the appropriate authorities?

Applying Whistleblower Protection Law to Snowden

Section 15(2) of the *SOIA* requires judges to undertake a two-step test and consider several factors when determining whether a person in Snowden's situation acted in the public interest. Section 15(3) requires a judge to first establish whether Snowden acted to disclose an offence that he reasonably believed had been or was about to be committed by another person, and then to balance the public interest in disclosure against the public interest in non-disclosure. Section 15(4) enumerates the factors that a judge must consider in assessing whether Snowden acted in the public interest when he released the documents, including:

> (a) whether the extent of the disclosure is no more than is reasonably necessary to disclose the alleged offence or prevent the commission or continuation of the alleged offence, as the case may be;
>
> (b) the seriousness of the alleged offence;
>
> (c) whether the person resorted to other reasonably accessible alternatives before making the disclosure and, in doing so, whether the person complied with any relevant guidelines, policies or laws that applied to the person;

(d) whether the person had reasonable grounds to believe that the disclosure would be in the public interest;

(e) the public interest intended to be served by the disclosure;

(f) the extent of the harm or risk of harm created by the disclosure; and

(g) the existence of exigent circumstances justifying the disclosure.

A methodical analysis of each branch of the test demonstrates why Snowden is unlikely to benefit from section 15.

The first branch of the test requires a judge to decide whether Snowden disclosed an offence that he reasonably believed was, was being, or was about to be violated. As noted in Part I, there is no law that expressly prohibits CSEC from conducting economic espionage. Thus, it would be difficult for Snowden to identify an offence under an Act of Parliament that was, was being, or was about to be violated by CSEC employees. This would preclude him from proceeding to the public interest balancing test.

This reality reveals a major flaw in the legislation. In an area as nebulous as national security law, it may be difficult for whistleblowers to pinpoint specific offences that were committed. Indeed, determining the legality of the Olympia program is hardly clear-cut for an experienced member of the legal community, let alone for an employee untrained in the law. Unfortunately, the result is that this provision may deter prospective whistleblowers from coming forward with information of serious public concern if they believe they will be automatically denied an opportunity to argue that their disclosure was in the public interest. Moreover, national security employees spearheading programs such as Olympia may infer that so long as their actions have a semblance of legality, they will continue to be shielded from public scrutiny.

To overcome this problem, Parliament ought to amend the first branch of section 15(2) in order to permit a judge to undertake a public interest balancing test so long as the whistleblower had reasonable grounds to believe that he or she was disclosing an offence committed by a CSEC employee. This would allow Snowden to argue that it was reasonable to believe that CSEC's mandate did not permit the agency to conduct operations such as Olympia and that there was a

reasonable basis for believing those responsible for the operation had acted contrary to Canadian law.

Irrespective of these policy concerns, Snowden would not be exculpated even if the court found that he disclosed an actual offence. Such a finding would merely permit the judge to proceed to the second branch of the public interest test. Under the second branch, Snowden would likely fail to demonstrate that the balance of indicia in section 15(4) favoured disclosure as well.

Sections 15(4)(b), (d), and (e): The Seriousness of the Alleged Offence, Reasonable Belief of Public Interest, and the Intended Public Interest Served

For starters, Snowden would be able to satisfy the considerations under section 15(4)(d) and (e) that he had reasonable grounds to believe that the disclosure was in the public interest, and that the intended public interest in disclosure was compelling. Given the vast extent of economic espionage and the potential public debate that such a revelation could provoke, a reasonable person in Snowden's position could have believed that the public would be well-served by knowing about CSEC's activities. The subsequent concerns expressed by government officials, media, and even Parliamentarians[44] demonstrated *ex facto* that disclosure served an important public purpose by sparking debate and accelerating calls for reform. Furthermore, Snowden could argue that the Canadian public had an interest in knowing the types of operations that CSEC undertakes pursuant to its mandate in order to enhance government accountability. The disclosure could (and, as it turned out, did) spark wider debates concerning whether economic espionage is something that an intelligence community agency should engage in, given its limited resources.

Granted, Snowden's leak of the Brazilian slideshow is not on the same scale as disclosing a wide-ranging data collection program, as existed in the US. Such an operation would entail potential infringements of section 8 *Charter* rights and would deserve thorough public scrutiny. However, the absence of a potential constitutional breach should not *prima facie* constitute sufficient grounds to

---

[44] "Hugh Segal decries 'zero legislative accountability' on spy activities", *Maclean's* (20 November 2013), online: <www.macleans.ca/news/canada/hugh-segal-decries-zero-legislative-accountability-on-spy-activities>.

invalidate the important public interest served in disclosing CSEC's activities, nor should it discount the seriousness of the alleged offence when weighing the merits of disclosure under section 15(4)(b). In fact, since CSEC's spying could have adverse impacts on Canadian economic actors and Canada's reputation abroad, the stakes for the Canadian public—and the economy—are high. In addition, the more intangible goals of public debate and transparency should not be discounted. Keeping this aspect of CSEC's mandate secret would diminish government accountability and would further shield the country's foreign affairs from public view. Furthermore, had a potential breach under the *NDA* been made out, a compromise of CSEC's mandate with widespread international implications would be an important consideration in weighing the seriousness of the alleged offence under 15(4)(b). In essence, Snowden "brought to light things that the public needed to know, and started a public debate that needed to happen."[45]

Sections 15(4)(a), (g), and (c): Extent of the Disclosure, its Exigency, and Reasonable Steps Taken to Avoid Disclosure

Snowden's public interest defence is most likely to fail when the judge considers whether the extent of the disclosure was no more than reasonably necessary to disclose the alleged offence, pursuant to section 15(4)(a). This requirement was not met. *The Globe and Mail* national security columnist Colin Freeze noted that he was not able to publish the full contents of the uncovered slideshow because it contained sensitive information, including names, phone numbers, and Internet Protocol addresses.[46] This finding suggests that the contents of the slideshow exposed more information than was necessary in order to corroborate the alleged illegal activity. If the information that Snowden revealed went beyond the mere identification of the program's existence, and therefore beyond what was reasonably necessary, it may very well tip the balance in favour of a public interest in non-disclosure.

---

[45] "Is Edward Snowden a Hero?", *The Globe and Mail* (8 November 2013), online: <www.theglobeandmail.com/globe-debate/editorials/is-edward-snowden-a-hero/article15354202>.

[46] Freeze, "Read a CSEC document", *supra* note 17.

Snowden also could not rely on a claim that exigent circumstances required the information to be disclosed. If Snowden uncovered ongoing violations of Canadians' rights or an act with the potential to cause serious bodily harm or death, a certain urgency to stop the continuing activity would be warranted. However, the contents of the slideshow were focused on methods of spying and were over a year old when they were released.[47] It is doubtful that a slideshow revealing economic intelligence-gathering methods would require urgent disclosure without more and, in any case, the need for urgent action would have likely passed by the time Snowden released the document a year later. Therefore, it is unlikely that Snowden could prove that its release was exigent under section 15(4)(g).

Finally, determining whether Snowden exhausted other reasonably accessible alternatives remains an open question. For instance, there is conflicting evidence as to whether Snowden raised his concerns with various NSA officials before going public.[48] Given this uncertainty, it is premature to determine whether the consideration under 15(4)(c) would operate in Snowden's favour.

Section 15(4)(f): Harm or Risk of Harm Caused by the Disclosure

The public interest served by disclosure, while significant, is unlikely to outweigh the harm that the disclosure caused, pursuant to section 15(4)(f). The government would argue that the harm was so damaging to Canada's long-term interests that the public interest favours the maintenance of secrecy. At a minimum, the risk of harm was significant, as the release of information pertaining to CSEC's operational techniques could jeopardize CSEC's future activities beyond Olympia and provide potential enemies with a window into the organization's operations. This type of information is generally guarded. CSIS,

---

47 *Ibid.*

48 In December 2013, the NSA issued a statement saying that there was no evidence Snowden revealed his concerns to officials prior to disclosing them to the public. In his testimony before the European Parliament, Snowden claimed to have spoken to 10 different officials about his concerns. See Andrea Peterson, "Snowden: I raised NSA concerns internally over 10 times before going rogue", *The Washington Post* (7 March 2014), online: <www.washingtonpost.com/blogs/the-switch/wp/2014/03/07/snowden-i-raised-nsa-concerns-internally-over-10-times-before-going-rogue>; Barton Gellman, "Edward Snowden, after months of NSA revelations, says his mission's accomplished", *The Washington Post* (23 December 2013), online: <www.washingtonpost.com/world/national-security/edward-snowden-after-months-of-nsa-revelations-says-his-missions-accomplished/2013/12/23/49fc36de-6c1c-11e3-a523-fe73f0ff6b8d_story.html>.

for its part, has developed categories of information that should not be disclosed; these guidelines were cited in *Almalki*.[49] Among these categories are information that identifies or tends to identify methods of operation or techniques, and information that identifies or tends to identify CSIS interests in individuals, groups, or issues.[50] The slideshow falls squarely within this definition because it details a potential economic espionage operation against a specific target. Thus, applying the CSIS rule would suggest that the disclosure caused substantial damage.

The potential to harm the public interest through this disclosure is even more pronounced in an international context. This type of disclosure could compromise Canada's reputation abroad by creating or furthering the perception that Canada is irresponsible in guarding its privileged information. When the courts have been asked to assess the merits of disclosing evidence under the *Canada Evidence Act,* they have taken into account the anticipated damage inflicted upon Canada's international relations. As noted by the Federal Court in *Canada v Ribic*, the release of sensitive information has the power to "make Canada's allies more reluctant to share intelligence in the future, thereby denying Canada access to vital information that would be required to protect civilians…"[51] However, a common-sense approach is required; not all information would seriously jeopardize Canada's reputation or national security if it were released publicly. As Justice Noel noted in *Canada (AG) v Canada (Commission of Inquiry into the Actions of Canadian Officials)*, the established practice of limiting disclosure for the sake of international relations cannot be overused to redact information that would have no serious impact on Canada's allies if it were released.[52]

---

[49] *Almalki*, *supra* note 11 at para 84. See also Mosley J's endorsement of the *Harkat* factors at paras 87–88 which provide "examples of information that *must* be kept confidential." Mosley J noted that while the factors are similar to the CSIS ones, the *Harkat* factors require that "harm *would* result from disclosure of the information." In this respect, risk of harm would not be sufficient [emphasis in original].

[50] *Ibid* at para 87. See also Forcese, *supra* note 10 at 419.

[51] *Canada (AG) v Ribic*, 2003 FCT 10 at para 18, 250 FTR 161.

[52] In the decision, Noel J rejected the government's request to withhold the name of the "CIA," arguing that the concerns of disclosure exaggerated the harm that could be done to US-Canadian relations. See *Canada (AG) v Canada (Commission of Inquiry into the Actions of Canadian Officials)*, 2009 FC 1317, 192 ACWS (3d) 1370.

However, Snowden is unlikely to benefit from such an approach because the information he revealed was operational. As University of Ottawa professor Wesley Wark suggests, it is improbable that the Olympia program was "made in Canada." Instead, it is more likely the result of a directive from the upper echelons of the so-called Five Eyes.[53] Under this exclusive alliance, Australia, Canada, New Zealand, the United Kingdom, and the US have agreed not to spy on each other and to work collaboratively by sharing intelligence derived from communication and electronic signals. A hypothetical court decision that afforded Snowden a defence would also have the effect of condoning the release of classified information. Considering that Canada receives more intelligence from the Five Eyes than it produces, endorsing such a disclosure could damage Canada's position within the alliance. An application of the judge's holding in *Ribic* suggests that Snowden's disclosure could negatively affect CSEC's abilities to work with its partners for the purpose of protecting the Canadian public.

Summary of Balancing Exercise

The various factors under section 15(4) must now be balanced. On one hand, Snowden would prevail in demonstrating that there were reasonable grounds to believe that the disclosure was in the public interest and that the intended public interest grounds were important. However, the government would likely succeed in demonstrating that Snowden's disclosures caused significant harm to Canada's national security apparatus and revealed more information than was reasonably necessary to expose the alleged offence. A further factor weighing against Snowden is that he released the information in the absence of exigent circumstances.

In light of the above observations, a court would probably find that the public interest in non-disclosure outweighs the public interest in disclosure. This is consistent with jurisprudence under the *Canada Evidence Act* public interest balancing test where courts have placed a premium on maintaining government

---

[53] Erica Alini, "Canada, Brazil and how snoops are threatening free trade", *Maclean's* (10 October 2013), online: <www.macleans.ca/economy/business/canadas-snooping-on-brazil-and-the-economics-of-cyber-espionage>; Wesley Wark, "Why is Canada spying on Brazilian industry? Time to examine priorities", *The Globe and Mail* (8 October 2013), online: <www.theglobeandmail.com/globe-debate/why-is-canada-spying-on-brazilian-industry-time-to-examine-priorities/article14731233>.

secrecy for the sake of protecting national security. The Supreme Court of Canada in *R v Carey* notes that the law has at times given virtually absolute priority to national security claims.[54] In *Ribic*, the court decided that a judge must resort to the means that are the least prejudicial to these interests in deciding to disclose information.[55] While the analysis under the *SOIA* calls for an *ex-post*, instead of *ex-ante,* review, the courts' heightened concern in endorsing the release of sensitive information would inform a section 15 analysis as well. Accordingly, the harm caused by the disclosures and Snowden's methods of releasing the information may be decisive in preventing him from successfully employing the public interest defence.

Given this conclusion, section 15 offers inadequate protection for prospective whistleblowers. While a judge is required to consider all the factors under section 15(4), there are no guidelines indicating how these factors are to be weighed. On a formal reading of the legislation, sufficient leverage is built into the balancing test in order to more heavily weigh the public interest for disclosure in some cases, such as when constitutional rights are at stake, while privileging the harm done to national security in other cases, such as when important operational information is released. Still, based on the precedents established in *Ribic*, national security interests may be prioritized over other interests. Thus, the efficacy of section 15 could be undermined if the provision is left to the courts without any guidance as to its application. If the considerations under section 15(4)(f) become more determinative than other factors, for instance, the entire balancing exercise may become a foregone conclusion.

It is laudable that the Canadian whistleblower provision provides a legal mechanism by which illegal activities can be brought to the public's attention. In that respect, the Canadian legislation better achieves the balance between government accountability and national security than its American counterpart.

---

[54] *Carey v Ontario*, [1986] 2 SCR 637 at para 22, 35 DLR (4th) 161. See also Steven Penney, "National Security Surveillance in an Age of Terror: Statutory Powers & Charter Limits" (2010) 48 Osgoode Hall LJ 247 at 281, which references the Supreme Court decision in *Canada (Prime Minister) v Khadr* to argue that on the whole, "courts have traditionally been reluctant to interfere with the executive's power in matters of national defence and foreign relations," so long as the activities do not interfere with the *Charter*.

[55] *Canada (AG) v Ribic*, 2003 FCA 246 at para 37, [2005] 1 FCR 33. The court also determined that deference is owed to the Minister when determining whether the disclosed information would be harmful at para 19. See also Forcese, *supra* note 10 at 407.

More important, however, is to what extent the legislation can actualize this balance, rather than simply being a false-promise to whistleblowers who depend on its provisions.

CONCLUSION

> "As loath as I am to give any credit to what's happened here, I think it's clear that some of the conversations this has generated, some of the debate, actually needed to happen… If there's a good side to this, maybe that's it."[56]
>
> —James Clapper, *Director of National Intelligence of the United States*

Since Snowden's leaks, the American and British governments have reportedly sought to rein in their respective security intelligence agencies. Prime Minister Stephen Harper commented that he was "very concerned" about revelations that CSEC was spying on the Brazilian government.[57] This may signal that some members of the Five Eyes recognize that the extent of their surveillance was misguided and perhaps even illegal. But as Oxford University Professor Timothy Garton Ash asks, "Would they be springing into action if not for the whistleblower and a free press?"[58]

This question underlies the debate over which public interest should take precedence: the interest in disclosing information or the interest in maintaining national security. As demonstrated above, CSEC's economic espionage in Brazil, as disclosed by Snowden, is most likely legal under Canadian law. While Snowden would be subject to the *SOIA*, he would not benefit from the *SOIA*'s public interest defence if he were tried in Canada. It is apparent from this analysis that the protections afforded to whistleblowers in the US are inadequate because American law does not admit any circumstance in which whistleblowers can

---

[56] Spencer Ackerman, "Fisa judge: Snowden's NSA disclosures triggered important spying debate", *The Guardian* (13 September 2013), online: <www.theguardian.com/world/2013/sep/13/edward-snowden-nsa-disclosures-judge>.

[57] "Harper 'very concerned' by Brazil spy scandal, vows follow up", *The Globe and Mail* (8 October 2013), online: <www.theglobeandmail.com/news/world/harper-very-concerned-by-canada-brazil-spy-scandal/article 14739556>.

[58] Timothy Garton Ash, "Government spying? Fear for yourself", *The Globe and Mail* (1 November 2013), online: <www.theglobeandmail.com/globe-debate/government-spying-worry-about-yourself/article 15190587>.

legally make illegal activities known to the public. In this respect, the Canadian system is far superior. Whistleblowers in Canada have a legal avenue to reveal secret information in the public interest; however, the public interest defence is not an easy threshold to meet.

Speaking from Russia in asylum, Snowden has stated that his biggest fear in releasing the classified information was that "nothing would change."[59] Time has proven Snowden's concern to be misplaced. Irrespective of the political and national security consequences of his disclosure, his case continues to compel legal commentators to seriously evaluate the parameters guiding security agencies and the protections afforded to whistleblowers. To paraphrase James Clapper, there is a good side to this, and that's it.

[59] Daniel Politi, "Julian Assange: Obama's Reforms to Surveillance Program Vindicate Snowden", *Slate* (10 August 2013), online: <www.slate.com/blogs/the_slatest/2013/08/10/julian_assange_obama_vindicates_snowden_by_changing_surveillance_program.html>.