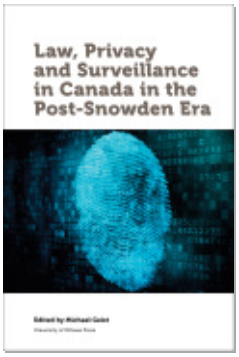
Law, Privacy and Surveillance in Canada in the Post-Snowden Era



Michael Geist, Wesley Wark

Published by University of Ottawa Press

Geist, Michael and Wesley Wark.
Law, Privacy and Surveillance in Canada in the Post-Snowden Era.
University of Ottawa Press, 2014.
Project MUSE.muse.jhu.edu/book/40610.

CHAPTER VII

The Failure of Official Accountability and the Rise of Guerrilla Accountability

Reg Whitaker

Introduction

When Edward Snowden fled his job as National Security Agency (NSA) contractor to exile in Russia, bringing with him millions of pages of secret documents that soon began appearing in media outlets around the world, the effect was that of a serially detonating bombshell.[1] There has been a great deal of debate about the meaning and significance of Snowden's revelations.[2] Much debate has turned on an apparent binary opposition between accountability and whistle-blowing.

Some would, of course, deny the very validity of the term "whistle-blower," calling Snowden simply a traitor deserving dire punishment, but this obfuscates the crucial distinction between spying and whistle-blowing. Espionage involves the transmission of state secrets to other states or hostile non-state actors to provide them with competitive advantage; whistle-blowers reveal state secrets to the public at large according to some (self-defined) concept of serving the public interest and/or following their own conscience. Whistle-blowing is inherently an illegal activity, yet its potential for serving the public interest has led to special whistle-blower protection laws in many jurisdictions.[3] Conventional spies may be fairly termed traitors for betraying their nation to another state or to violent non-state actors. The moral culpability of whistle-blowers must be unwrapped

from the context of their illegal actions. Motive is crucial. Even if one rejects, in part or in whole, the self-justifying rationale the whistle-blower offers for his or her acts, the fact remains that a disinterested motive distinguishes the whistle-blower from the spy. While legal sanctions may be appropriately applied to the law-breaking whistle-blower, the consequences of his or her unauthorized disclosures will be very different from the consequences of espionage. They may even be positive.

Snowden the whistle-blower, it is widely conceded, has raised questions to which the existing accountability mechanisms have failed to provide satisfactory answers, or in many cases any answers at all. Although the United States continues to demand Snowden's return from Russia to face legal charges, the President has in effect responded to Snowden's whistle-blowing message with a wide-ranging package of reforms circumscribing NSA activities and enhancing external controls over the agency's operations. The US Appeals Court dealt a potentially even more damaging blow when, in May 2015, it ruled the NSA bulk collection program illegal.[4] *Pro forma* denials that these changes have been prompted solely by the Snowden leaks are believed by no one. In other words, Snowden the whistle-blower has paradoxically prompted both legal action against himself and a policy response that recognizes the *de facto* legitimacy of the rationale that lay behind his illegal actions.

This is a very troubling observation, especially for those with a stake in the existing national security institutions. Stakeholders in a sense include all the citizenry that wishes to be protected from terrorist acts, but it applies particularly to those officials who themselves have access to secret information, who are thus implicated in a system the shortcomings and dangers of which have been exposed by Snowden's leaks — and recognized as being well-founded at the highest levels of the American government.

Improved Official Accountability

A way out of this moral dilemma has been posed as improved official accountability. Snowden's leaks may have revealed problems, but his methods cannot be condoned. Therefore the answer must be found in responsible legitimate accountability replacing irresponsible, self-elected, self-justifying leakers. That was the core of President Obama's message on NSA reform. In Canada, the Harper

government, as well as its national security agencies and their review bodies, have been blithely dismissive of concerns about the Canadian NSA equivalent, the Communications Security Establishment (CSE).[5] Unofficial calls for reform from lawyers and academics to privacy commissioners — although differing in detail — have all echoed the same broad policy prescription: strengthened official accountability mechanisms must be put in place that will reduce or obviate the need for more Snowden-like leaks.

As someone who has long advocated improved accountability in national security matters, I have no inclination to challenge the overall thrust of these calls for reform. Strengthened accountability mechanisms and stronger leadership of the review and oversight bodies should, if properly conceived and managed, contribute both to strengthening civil liberties, privacy rights and the rule of law, as well as contributing to effective national security and public safety. I do, however, think that the problems revealed by the Snowden revelations point to difficulties more complex and unsettling than are encompassed in the formula "Better accountability is the answer to whistle-blowers."

I would argue that the very need for, and existence of, whistle-blowers is rooted in the inherent limitations and inadequacies of existing mechanisms of accountability. Snowden, and leakers such as Bradley (now Chelsea) Manning, arise because of, not in spite of, existing accountability. Indeed, what Snowden has done can be understood as a form of "guerrilla accountability" that arises in the absence of effective official or orthodox forms of accountability.[6] I will further argue that there is good reason to believe that these inherent limitations in official accountability almost guarantee future whistle-blowers, even with reformed institutions. Accountability and whistle-blowing may thus be ensnared in a struggle with one another that may have no resolution in the foreseeable future.

Snowden, it must be said, is hardly a one-off (even when his actions are grouped with the earlier Manning WikiLeaks disclosures). It is historically striking how much critical information about the abuse of national security secrecy has been revealed by deliberate unauthorized disclosure, and how very little by official accountability. There is the celebrated precedent of Daniel Ellsberg's Pentagon Papers leaks in 1971, which blew the lid off the US government's secret wars in Southeast Asia, and which revealed publicly that the government had systematically lied about its activities, not only to

the public but also to Congress, rendering ineffective legislative oversight of American covert activities abroad.

The now notorious COINTELPRO program, comprising often illegal projects conducted by J. Edgar Hoover's FBI aimed at infiltrating, discrediting, and disrupting domestic political activities, was revealed only when a group styling itself the "Citizens' Commission to Investigate the FBI" broke into an FBI field office in Pennsylvania, stealing documents that exposed the program when passed to media outlets. Facing a storm of public opprobrium, Hoover declared within a year that the once super-secret program — which had entirely escaped Congressional notice — was to be shut down.

Why are official accountability channels relatively ineffective in catching the really big problems in national security? There are multiple answers to this question, but a major one is regulatory capture, a phenomenon well known and amply described in public policy literature.[7] This explains how the gamekeeper turns poacher, the process by which a regulatory agency, formed to act in the public's interest, ends by serving the interests of the industry it is supposed to be regulating, rather than the public.

Among factors contributing to the prevalence of regulatory capture, one stands out for our purposes: *control over information*. Even in areas remote from national security concerns, the capacity of a regulated industry to control or influence the flow of information, which the regulatory body requires to perform its functions, is an important part of the regulated industry's ability to capture or tame its regulator. In national security, the greatly enhanced, indeed sometimes exclusive control by the agencies of national security information imposes a double bind on review or oversight bodies. Secrecy is a crucial bureaucratic resource that can yield power and relative autonomy to the bureaucratic actors with privileged access to secret information, both within the executive and in relation to the legislature and the public. National security review bodies require unrestricted access to the agencies' secrets in order to perform their oversight functions. But this is rarely granted in full, for a variety of more or less plausible reasons, such as the understandable reluctance of agencies to permit real-time intrusive surveillance of their ongoing operations. Sympathetic to this concern, review bodies generally refrain from attempting to scrutinize ongoing operations, concentrating instead on *post hoc review*.[8] This restraint however leaves

open-ended the question of how the term "operational" is defined, and leaves the definition in the hands of the agencies.

Varying from jurisdiction to jurisdiction, in practice there are a number of constraints on access to information crucial to carrying out the review function (I will refer to more specifics below). While not necessarily fatal — except in the cases of particularly dysfunctional or toothless bodies such as the RCMP Public Complaints Commission — these constraints do impede the capacity of review bodies to escape some degree of regulatory capture.

It is the second part of the double bind on secrecy that is especially telling for the weakness of official review/oversight. Let us assume for a moment that a review body does have almost total command over pertinent information, including more or less unrestricted access to as wide a range of secret intelligence as allows it to make definitive judgment on the performance and behaviour of the agency in question. At this point a paradox emerges: the greater the access to secrets the review body has gained, the less it will be able to provide a substantive degree of transparency to Parliament and public.

Access to secrets places the review body inside the loop of national security confidentiality. But this is an enchanted circle from which the "external" review body can never fully return. In the ancient Greek myth Persephone, daughter of Demeter, goddess of the sunlit fields, was obliged to remain for part of every year in the dark Underworld with her abductor Hades because she had eaten seven seeds of a pomegranate from the land of the dead. So too review bodies, having tasted the secrets, must remain forever partially in the shadows. When they return to tell their stories, the public tends to see their narratives as thin, opaque, and dull. Which in truth they often are, once shorn of the secret information that would provide substance and credibility.

When the US Director of National Intelligence (DNI) James Clapper told a Congressional committee in March 2013 that the NSA does not collect any type of data at all on Americans, there were members of the House and Senate intelligence committees who knew this to be untrue but were unable (or unwilling) to break their commitment to secrecy. One senator's aides have claimed that they privately alerted Clapper's office to his error and unsuccessfully requested a correction of the public record.[9] It took the leaks of the whistle-blower Snowden, in safe refuge in Russia, to reveal publicly

that the DNI had in fact lied to Congress and the American people. Faced with this embarrassment, Clapper initially said that he had provided the "least untruthful" answer he could in a public setting. Finally, with calls for perjury charges on the horizon, Clapper blurted out:

> I probably shouldn't say this, but I will. Had we been transparent about this from the outset right after 9/11 — which is the genesis of the 215 program [bulk data collection] — and said both to the American people and to their elected representatives, we need to cover this gap, we need to make sure this never happens to us again, so here is what we are going to set up, here is how it's going to work, and why we have to do it, and here are the safeguards… We wouldn't have had the problem we had.[10]

That transparency would have whisked away problems with an inherently problematic program is doubtful, but if so, Clapper's second (or third) thoughts actually constitute an indictment of the existing system: the agencies initiate in secret a legally dubious program; official accountability fails to bring the agencies to account and even contributes to a cover-up; an illegal leaker breaks the cover, revealing official deception; in the face of which the official ultimately responsible admits that the program should never have been carried out in secret in the first place. Of course, without the illegal leak, none of this would have been revealed and the apology would never have happened. And no reform of this deeply flawed system would ever have been contemplated.

The Three Basic Rules of Secrecy

The Clapper incident represents in microcosm the accountability/whistle-blowing conundrum. Official accountability failed to work because the oversight body — in this case Congress — was trapped by the same rules against disclosure of secrets that govern the agencies. It is worth paying close attention to these rules and how they are enforced to gain some appreciation of the difficulties that face even honest attempts at accountability reform.

If we briefly review the specific arguments that have been made in favour of secrecy in security and intelligence, we come upon an obvious and, in a way, unassailable, objection to any critical attack on privileged access to secrecy. The arguments for secrecy are

reasonable and logical. Broadly speaking, they break down into three broad categories of information that cannot be publicly disclosed. These may be referred to as the three basic rules of secrecy:

1. No disclosure of the identification of secret sources of intelligence.
2. No disclosure of methods and techniques of covert operations.
3. No disclosure of information received in confidence from foreign governments or agencies.

Clearly these are all perfectly reasonable grounds for non-disclosure. No agency could operate covertly if its secret sources were publicly identified. No covert agency could operate effectively, or at all, if its methods were transparent to the very targets of its operations. And failure to secure information received in confidence from abroad would quickly lead to the damaging loss of access to such information. These three rules are, I believe, the core rationale for the exercise of secrecy in security and intelligence, and can stand alone without the cloak of particular legal sanction, and outside the peculiarities of different political systems, whether parliamentary or presidential. I do not intend to challenge these grounds, in themselves, although their interpretation in specific cases is quite another matter.

If we grant that these are all reasonable qualifications for secrecy, and that a serious breach in any one of these would fail an appropriate injury test, are we further contending that legitimate requirements for secrecy undermine or make impossible democratic responsibility in national security matters? Not quite. First, the claims for secrecy advanced by those within the national security loop cannot be taken at face value, and always require critical scrutiny from outside the loop. We start with a brief look at possible limitations on the three rules of secrecy.

On Rule 1: The core rationale for the rule is valid, but it is too often interpreted in a manner so expansive as to lose much of its legitimate force. Example: information is withheld that is purely contextual, rather than directly contributing to the identification of a secret source. The justification for this is that any smart journalist or, worse, the targeted organization or network, could deduce from contextual information the identity of a source. While this could be the case, sometimes so much non-specific contextual information is

withheld that effective *public* accountability regarding the efficacy and/or propriety of intelligence sources is impossible. In such cases, too much trust must be accorded review/oversight agencies reporting in secret to the very governments they are reviewing. "Trust us" becomes a motto that has to be extended from the watchers to those who watch the watchers, something not always possible in all cases for a rightly sceptical media, political opposition, and public.

On Rule 2: Anyone who has been involved in declassification requests whether for scholarship, journalism, or in court proceedings or quasi-judicial hearings, will be aware of the so-called mosaic argument for non-disclosure. To critics on the outside of classification decisions, this is often seen as a ruse whereby virtually any and all information about the secret agencies is denied. The argument goes like this: small bits of information, however innocuous in themselves, could be put together by hostile forces to form a mosaic picture of methods and techniques of operation, and of targets. While this had some validity during the Cold War, when Soviet intelligence, for instance, could be assumed to seize with loving attention every tidbit that might deepen their knowledge of their professional adversary, it seems less compelling in the era of the war on terror, when networks or even nodes of non-state actors spring up, form, and reform more or less spontaneously with or without a great deal of continuity, and certainly without close central direction.

In any event, the mosaic effect is stretched beyond all reasonable bounds again and again. A recent example is afforded by Mr. Justice O'Connor's inquiry into the Maher Arar affair.[11] When early in its investigation, the Commission tried to make public a suitably sanitized summary of *in camera* Canadian Security Intelligence Service (CSIS) testimony, the government demanded major cuts and signalled its intention to contest the matter before the Federal Court, if necessary. Among the bits the government insisted should be excised was a reference to the startling fact that CSIS keeps files on suspected terrorists: surely *a reductio ad absurdum* of the mosaic effect![12] O'Connor chose at this stage of his inquiry not to contest the censorship, but when his final report was published, a number of excisions insisted upon by the government were later contested in the Federal Court and many, although not all, were ordered disclosed.[13] Threat of recourse to the courts forced additional disclosure of material published by another post-9/11 inquiry, Mr. Justice Iacobucci's inquiry into Messrs. Almalki, Elmaati, and Nureddin.[14]

It should be made clear that the additional information disclosed by court order in these two Canadian cases did not radically transform public understanding of the facts — in some instances it merely illustrated how inane some of the non-disclosure decisions were in the first place (that leading US intelligence agencies are called the "CIA" and the "FBI" was apparently judged a state secret!). More telling is that the commissions had already exercised prior self-censorship of the public report in anticipation of redactions to be applied. Even more to the point, public inquiries are one-off events. Official review bodies, always concerned about their ongoing working relationship with the agencies they review and deeply concerned to maintain their own legitimacy as players in the national security world, rarely contest the application of the government's expansive interpretation of non-disclosure in public reports of information deemed to fall under national security confidentiality. Judges are not brought into this process, unless the entire system has fallen into serious crisis (this has not yet happened anywhere to my knowledge). Thus interpretations of non-disclosure are normally subject to no third-party review beyond the agencies and the review bodies acting in concert. Until, that is, someone blows a whistle.

Whatever concerns are raised by close attention to the actual application of the first two rules, the Snowden revelations unequivocally point to the misuse and abuse of Rule 3 as crucial in understanding the failure of official accountability and the necessity of guerrilla accountability.

On Rule 3: The longer I have watched the operation of official secrecy in the name of national security, the more I have become convinced that the foreign confidence argument might better be called the foreign confidence trick. Of course, intelligence received in confidence from foreign sources cannot be splashed about without consequences. Yet the question that should be addressed, but almost never can be, is this: what criteria are being applied when caveats and restrictions are stamped on intelligence exchanged between allies? How do we know that this process is not part of a "you scratch my back, I'll scratch yours" operation of mutual convenience whereby allied governments and sister agencies simply cover for each other and prevent disclosure in each country by mutual consent — call it "information laundering." Conspiratorial suspicion should be resisted, but it is hard when the very bodies that are supposed to review and hold the agencies accountable may themselves be

prevented from seeing information that is so laundered by international agreement.

Let me provide an example of this latter problem drawn from the experience of the strongest of Canadian review bodies, the Security Intelligence Review Committee (SIRC). In 1988, while still under the aggressive leadership of its first Chair, Ron Atkey, who never shrank from public tangles with CSIS, SIRC entered into a "third-party access protocol" with CSIS whereby the latter agency undertook, to the best of its ability, to gain the consent of foreign entities to disclose to SIRC documents originating from those entities that SIRC believed necessary for its investigations of CSIS activity.[15] There were, however, no guarantees provided, despite SIRC's clear mandate to "have access to any information under the control of the Service."[16] It is not known publicly how much, if any, foreign-origin documentation has actually been withheld from SIRC over the years, because such information itself cannot, of course, be disclosed under national security confidentiality. In the mid-1990s SIRC did publicly complain that a document it had sought was instead returned by CSIS to its foreign donor.[17]

A crucial fact about the Snowden revelations is that they disclose surveillance activities primarily by the NSA, but also by the NSA's main foreign counterparts in the so-called Five Eyes signals intelligence alliance — the "Anglosphere" of intelligence exchange and cooperation —, the United Kingdom (senior partner) and three junior partners: Canada, Australia, and New Zealand.[18] Intelligence collected is shared community-wide; targets of Five Eyes surveillance are global in scope. While the lead agencies operating within the alliance (NSA, Britain's Government Communications Headquarters [GCHQ], CSE) are national in origin and under national legal jurisdiction in the first instance, their operations as allies are enthusiastically *sans frontières*. Their respective review/oversight bodies, on the other hand, are anchored — one might cynically suggest, imprisoned — within their national jurisdictions. None of the review bodies have the capacity to track a trail of accountability past their own national agencies. Even in the name of public interest accountability they have no right and no means to compel the production of information of foreign origin.

A Call for Guerrilla Accountability

This has serious implications for their capacity to fulfill even their statutory requirements to review domestic operations. It has been widely conjectured that the Five Eyes partners may have organized end runs around their own publicly professed attestations that they never spy on their citizens, only on foreigners. This reportedly involves doing each other's intelligence laundry: GCHQ might do some spying on Canadians in exchange for CSE undertaking some surveillance in Britain, in which case, no domestic laws are broken, and no one is the wiser. All the allies have always denied this charge, but following the Snowden revelations, public trust in Clapper-like official assurances of legality and propriety has been eroded. The point is that official accountability mechanisms will not, and indeed, cannot provide any reassurance that information laundering is not taking place since none of the existing mechanisms can follow the trail across national boundaries. There is a clear call here for guerrilla accountability to do what official accountability cannot.

Another example: CSIS was granted permission by the Federal Court in 2009 to spy on Canadians abroad, but the judge who gave that permission, Richard Mosley, later discovered that CSIS had overstepped legality by asking CSE to task their foreign partners with this assignment. CSIS and its lawyers had in effect lied to the court "about their intention to seek the assistance of the foreign partners," raising questions of exposing Canadians to human rights abuses.[19] "This would," he went on, "involve the breach of international law by the requested second parties."[20] A CSE official "candidly" admitted that his evidence in support of the original warrant application had been "crafted" with legal counsel to exclude any reference to plans to use second parties. Worse yet, Mosley indicated that the Deputy Attorney General of Canada had argued "that the Court should be kept in the dark about matters it may have reason to be concerned about if it was made aware of them."[21] Ironically, Mosley, an unusually vigilant and sceptical judge, was alerted to the problem by close reading of information in reports from SIRC and the CSE Commissioner. Yet these same review bodies had not flagged any suspicions. It was fortuitous that Mosley alone, from his uniquely strategic position in this case, could compel testimony that revealed deception of the court. On their own, the review bodies had neither the will nor the means to raise a finger of protest. A justice of the

Federal Court was, in a curious sense, providing the necessary guerrilla accountability to blow the whistle.

The government's response was to appeal Mosley's decision. This failed at the Federal Court of Appeal, but undeterred, the government has taken its appeal to the Supreme Court.[22] Whatever the outcome at the highest court, in late 2014 the government passed Bill C-44, amending the *Canadian Security Intelligence Service Act*, through the House of Commons. C-44 specifically authorizes CSIS under warrant to outsource its intelligence collection abroad.[23] This will effectively place its external intelligence collection out of the reach of any Canadian oversight, precluding for instance any critical notice of the use of intelligence derived from torture or other methods abusive of human rights against Canadian citizens.

O'Connor, in the second part of his Arar Report, made extensive recommendations for strengthening accountability in the light of what had happened to the unfortunate Mr. Arar at the hands of the American extraordinary rendition program and outsourced Syrian torturers. Central to his reform plan was the observation that in the face of a globalized terrorist threat post–9/11, counterterrorism operations were being integrated, across institutional stovepipes like CSIS and the RCMP, across federal-provincial jurisdictional boundaries and, most importantly, across national boundaries between allies and cooperating states.[24] Accountability should also be better integrated to match the growing integration of counterterrorism efforts; otherwise accountability would fall far behind the greatly increased legal and operational power of the agencies. A number of government agencies with national security responsibilities have inadequate oversight, and in some cases, such as the Canada Border Services Agency, no external accountability whatsoever. O'Connor recommended bringing them all together under integrated mechanisms of external scrutiny. Almost eight years later, the government response has been zero. Actually, less than zero. They have abolished one of the two main oversight bodies for CSIS, the Inspector General.[25] SIRC is in the midst of a leadership crisis, with the former Harper-appointed chair, Arthur Porter, facing extradition from Panama on multi-million dollar fraud charges, while his successor was forced to step down for possible conflict of interest.[26] While still the potentially most effective review body in Ottawa, SIRC has seen its resources flatlined over the past decade, and its staff resources diminished while CSIS has been expanding steadily in size and resources.[27] Nor have there

been any official moves to create a parliamentary national security and intelligence committee.

In any event, not even O'Connor's recommendations for more integrated accountability mechanisms would touch on the international dimension. Indeed, even though Arar was a victim of counterterrorism across borders, the inquiry into his case was strictly limited to the complicity of Canadian officials with the behaviour of a foreign government that was itself beyond the jurisdiction of a Canadian inquiry. American officials, the real authors of Arar's kidnapping and detention abroad, could be neither the object of the inquiry nor compelled to appear as witnesses. Even if greater integration of accountability were to be achieved in Canada, there is no legal or political basis at present for the extension of that integration across national boundaries. In this era of borderless terrorist networks and borderless counterterrorism operations, this is tantamount to saying that much, if not most, of what goes on in the world of security and intelligence is effectively beyond the reach of nationally based official accountability to bring transparency — leaving an important opening for guerrilla forms.

It is precisely this international dimension that has been dramatically opened up by the Snowden revelations. As indicated earlier, Snowden's disclosures have shed light not only on the impact of the operations of the NSA on American citizens, but on the impact of NSA surveillance on governments and people across the world, and on the global reach of the Five Eyes alliance. Snowden's disclosures have had particular impact on Canada, revealing not only that Canada spies on other countries, like Brazil (perhaps out of alliance obligations, perhaps for its own economic espionage purposes); but more pointedly, revealing hard evidence of CSE intelligence collection on Canadian citizens, which it has always denied.[28] CSE has admitted that it does collect metadata on Canadian communications, although the Prime Minister has denied it.[29] The former CSE chief tried to square the circle by arguing before a parliamentary committee that metadata did not constitute "communication" under the law.[30] Claims that metadata do not constitute "real" data, "just the address on the envelope, not the letter inside," are deeply misleading. The Privacy Commissioner has suggested that "metadata can sometimes be more revealing than content itself."[31] The revelation that metadata is being collected on Canadians under unspecified parameters has led the British Columbia Civil Liberties Association to launch a lawsuit

against CSE claiming that its "secret and unchecked surveillance of Canadians is unconstitutional,"[32] a lawsuit that at the very least is designed to open CSE's collection practices to greater transparency, and has won widespread approval.[33] Even the former CSE chief suggested that the agency should be put under the scrutiny of a parliamentary committee "to make Canadians more knowledgeable about what the intelligence agencies are trying to do on their behalf."[34]

Of course, the very knowledge that CSE *might* be violating the rights of Canadians would never have come to light without the guerrilla accountability of Edward Snowden.

That a serious official accountability deficit exists in Canada was spotlighted in early 2015 when the government introduced sweeping revisions to its anti-terrorism powers in Bill C-51, *The Anti-Terrorism Act, 2015*.[35] Among other things, this legislation hugely widens the definition of what might be encompassed under the category of "terrorist" activity; greatly expands the information-sharing capacity of the federal government; expands the boundaries of the no-fly list; extends the length of preventive detention while lowering the threshold conditions; creates new criminal offences for promoting or advocating terrorism (including "terrorism in general"); and enables CSIS to apply secretly for judicial "disruption" warrants that would permit CSIS agents to break Canadian law and violate *Charter* rights with impunity. This dramatic proposed expansion of intrusive state powers into civil society would be accompanied by not one improvement on the already failing and grossly inadequate accountability system. In its defence, government spokespersons stretched credulity by claiming that SIRC already provides "robust" accountability. It also made the odd claim that greater "judicial oversight" arises out of C-51, even though the disruption warrants actually constitute secret judicial enabling of law-breaking, making judges agents of the executive rather than overseers of the legal propriety of government actions.

C-51 has roused a storm of criticism,[36] much of it focussing on the lack of oversight over the newly empowered security agencies. The NDP and Green parties opposed and vowed to repeal C-51, and while the Liberals voted in favour of what they termed a flawed bill, this was with the caveat that if elected they would add effective oversight. Most strikingly, an open letter, signed by four former prime ministers, five retired Supreme Court justices, three former Ministers of Justice, four former Solicitors General, three former members of

SIRC, and former privacy and RCMP complaints commissioners, called for "independent oversight and effective review mechanisms [to] help ensure that resources devoted to national security activities are being utilized effectively and efficiently," as well as to prevent abuses of human rights.[37]

Given the government's majority in both houses of Parliament, and its consistent refusal to consider enhanced accountability, C-51 is likely to become law, more or less in its initial form. However much it might be improved by strengthened parliamentary and other forms of oversight and review, the limitations of formal accountability must be kept in mind. C-51 actually poses new limits on any external review. For instance, disruption warrants would be issued in such secrecy that they could very likely never come to the attention even of the intended targets and would equip CSIS in advance with judicially mandated "get out of jail free" cards that obviate any external scrutiny: it is unclear what oversight could oversee in such cases. Finally there is the all-too familiar problem already experienced in Canada and elsewhere, as described earlier, that oversight in secrecy is, in so many ways, oversight denied.

Nor should we look only to potential impropriety in the actions of the empowered national security agencies. Serious questions have been raised about the potential for renewed turf wars between the RCMP and CSIS, and the potential for CSIS actions impeding the capacity of the RCMP as a law enforcement agency to bring successful criminal cases.[38] The ballooning definitions of "terrorism" risk expanding the scope of surveillance and, now, disruption to groups such as First Nations and environmentalists protesting pipeline projects. This could potentially lead to the loss of social licence for CSIS and the RCMP, which would be counterproductive for fighting terrorism. Official accountability will be severely stretched to deal with these challenges, and particularly severely stretched to deal *publicly* with these challenges. Hence, the continued need for guerrilla accountability.

If Snowden guerrilla accountability alone exposed possible CSE excesses, how much greater will the need be for guerrilla accountability in a Canadian national security world governed by C-51. The Privacy Commissioner, Daniel Therrien, has weighed into the debate over C-51 with a strong warning about the almost unrestricted information sharing envisaged in the proposed legislation, which he terms "excessive," along with privacy safeguards that he finds

"seriously deficient." "History," he points out, "has shown us that serious rights abuses can occur in the name of national security." He goes on to explain that "revelations by US whistle-blower Edward Snowden have shown how pervasive government surveillance programs can become."[39]

It is thus with some irony that Edward Snowden himself, via video link from his exile in Moscow, should warn Canadians that their country has one of the "weakest oversight" frameworks for intelligence gathering in the Western world. He called C-51 "an emulation of the *USA PATRIOT Act*" (not a complement) and went on to point out the critical importance of real accountability in protecting liberal freedoms when under pressure from the national security state.[40]

There has never been a Canadian Snowden. There have been rare examples of disgruntled ex-employees or ex-agents seeking journalistic outreach to make their concerns known,[41] but never whistle-blowers in place. Whether this will remain true in the future is a matter of conjecture.

Conclusion

Observers seeking to strike a reasonable balance between the need for effective security on the one hand and concern for the rule of law, privacy rights and the protection of liberal democracy on the other, will be uncomfortable with the idea of promoting illegal leakers as an answer to ineffective official accountability. While Snowden has provided moderate and reasonable arguments to support his actions, and his journalistic partners — *The Guardian*, *The Washington Post* and Glenn Greenwald — have been responsible in what they have released, there are of course no grounds for assuming that the next Snowden will have appropriate motives for breaking the law, and breaking the trust placed in him to access secret information. Leakers aspiring to the title of whistle-blower may be moved by private resentments; they may be on ego trips; they may be under extreme ideological direction; they may be just plain deranged. Yet unless truly radical revisions in how official accountability is allowed to operate are implemented — most importantly including the expansion of its scope to the international dimension —it is certain that if the powerful spy agencies are to be held to account and to operate under the rule of law, guerrilla accountability will remain a necessary part of the process.

Notes

1. For background on the Snowden affair, see Luke Harding, *The Snowden Files: The Inside Story of the World's Most Wanted Man* (London: Guardian Books, 2014).
2. The case for Snowden is made by his journalistic collaborator, Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the U.S. Surveillance State* (Toronto: McClelland & Stewart, 2014). Alarmist claims by officials about profound damage to national security — even lives lost — are assessed by Shane Harris, "The Snowden Aftermath (Revised): Intelligence Leaks May Have Caused Damage but It's Not Irreparable" *Foreign Policy* (11 July 2014).
3. Rahul Sagar, *Secrets and Leaks: The Dilemma of State Secrecy* (Princeton, NJ: Princeton University Press, 2013) points to an intermediate category of leaker who discloses classified information under the cloak of anonymity. A whistle-blower is a leaker whose identity is made known to his or her employer. When Snowden chose to make his identity public he moved from leaker to whistle-blower.
4. "President Obama's Speech on NSA Surveillance Reforms — Full Text," *Guardian*, 17 January 2014, <http://www.theguardian.com/world/2014/jan/17/obama-speech-nsa-surveillance-reforms-full-text>. United States Court Of Appeals for the Second Circuit, August Term, 2014, Docket No. 14-42-cv, American Civil Liberties Union et al v. James R. Clapper & Michael S. Rogers.
5. See denials by CSE Chief John Foster in testimony to the Standing Senate Committee on National Security And Defence (3 February 2014), "Stephen Harper Says Canadians' Metadata Not Collected," Toronto Star, 26 February 2014, <http://www.thestar.com/news/canada/2014/09/26/stephen_harper_says_canadians_metadata_not_collected.html>. See also Stewart Bell, "Stephen Harper's Top Security Advisor Denies Reports of Illegal Spying on Canadians Using Airport Wi-Fi," *National Post*, 3 February 2014, <http://news.nationalpost.com/news/canada/harpers-top-security-advisor-denies-illegal-eavesdropping-of-canadian-travelers-using-airport-wi-fi>.
6. See *Brazil*, DVD (1985; Universal City, CA: Universal Studios, 1998), Terry Gilliam's British dystopian film, a reworking of Orwell's *1984*, where Robert De Niro plays a self-described "guerrilla repairman" who quits the incompetent if not malevolent official repair agency and now intercepts distress calls to his former agency and makes repairs properly before government agents arrive to wreak havoc. This captures something of the self-image of Snowden-style guerrilla accountability.
7. Michael E Levine & Jennifer L Forrence, "Regulatory Capture, Public Interest, and the Public Agenda: Toward a Synthesis" (1990) 6:1 *Journal of Law, Economics & Organization* 167.

8. "Oversight" is often used as denoting scrutiny of operations in real time, while "review" is defined as only after the fact. I have used both terms here interchangeably as review is an element of oversight.
9. Aaron Blake, "Sen. Wyden: Clapper Didn't Give 'Straight Answer' on NSA Programs," *Washington Post*, 11 June 2013, <http://www.washingtonpost.com/blogs/post-politics/wp/2013/06/11/sen-wyden-clapper-didnt-give-straight-answer-on-nsa-programs/>; David Cole, "The Three Leakers and What to Do About Them," *New York Review of Books*, 6 February 2014, <http://www.nybooks.com/articles/archives/2014/feb/06/three-leakers-and-what-do-about-them/>.
10. Spencer Ackerman, "US Intelligence Chief: NSA Should Have Been More Open About Data Collection," *The Guardian*, 18 February 2014, <http://www.theguardian.com/world/2014/feb/18/us-intelligence-chief-nsa-open-bulk-phone-collection>.
11. Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar* (Ottawa: Public Works and Government Services Canada, 2006) , <http://www.sirc-csars.gc.ca/pdfs/cm_arar_bgv1-eng.pdf>.
12. I am drawing here on my experience as an adviser to O'Connor at the Arar inquiry. See Reg Whitaker, "Arar: the Affair, the Inquiry, the Aftermath," Institute for Research on Public Policy, *Policy Matters* (May 2008) 9:1.
13. Federal Court of Canada DES-4-06, Attorney General of Canada and the Commission of Inquiry (24 July 2007).
14. The Honourable Frank Iacobucci, *Internal Inquiry into the Actions of Canadian Officials in Relation to Abdullah Almalki, Ahmad Abou-Elmati and Muayyed Nureddin* (Ottawa: Public Works and Government Services, 2008) and "Supplement to the Public Report" (2010).
15. Memorandum from Ron Atkey, Chair of Security Intelligence Review Committee to J Reid Morden, Canadian Security Intelligence Service Director (25 May 1988) with Annex of same date, disclosed under Access to Information Request to SIRC, 23 January 1995.
16. *Canadian Security Intelligence Service Act*, R.S.C. 1985, c. C-23, s. 39(2). S. 39(3) indicates that apart from Cabinet confidences, "No information described in subsection (2)… may be withheld from the Committee on any grounds."
17. Canada, Security Intelligence Review Committee, *Annual Report 1995-1996* (Ottawa: Public Works and Government Services Canada, 1996) at 5–6.
18. A quick introduction to the Five Eyes is Paul Farrell, "History of 5-Eyes — Explainer," *The Guardian*, 2 December 2013, <http://www.theguardian.com/world/2013/dec/02/history-of-5-eyes-explainer>.
19. *X (Re)* 2013 FC 1275, 69 DLR (4th) 157 at para. 90.

20. *Ibid.* at para. 105.
21. *Ibid.* at para. 89.
22. Jim Bronskill, "Overseas CSIS Terror Tracking Case to be Heard by Supreme Court," *The Canadian Press*, 5 February 2015, <http://www.cbc.ca/news/politics/overseas-csis-terror-tracking-case-to-be-heard-by-supreme-court-1.2946162>.
23. Bill C-44, *An Act to amend the Canadian Security Intelligence Service Act and other Acts*, 2d Sess, 41st Parl, 2014, s. 8(1).
24. Canada, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006).
25. Jim Bronskill, "Axing CSIS Watchdog 'Huge Loss,' Says Former Inspector General," *The Canadian Press*, 9 August 2012, <http://www.cbc.ca/news/politics/axing-csis-watchdog-huge-loss-says-former-inspector-general-1.1143212>.
26. "Arthur Porter, ex-McGill Hospital Director, to be Extradited from Panama," CBC News, 17 January 2015, <http://www.cbc.ca/news/canada/montreal/arthur-porter-ex-mcgill-hospital-director-to-be-extradited-from-panama-1.2916610>. His successor, former cabinet minister Chuck Strahl, felt compelled to step down in the face of criticism of his connections with the Enbridge pipeline corporation at a time when anti-pipeline protestors were complaining of CSIS surveillance of their activities. Chris Plecash & Mark Burgess, "Tougher Conflict of Interest Act Needed Following SIRC Controversy Say Experts," *Hill Times*, 2 March 2014, <http://www.hilltimes.com/news/news/2014/02/03/tougher-conflict-of-interest-act-needed-following-sirc-controversy-say-experts/37318>.
27. Chris Hall, "CSIS Watchdog Agency Starved of Staff, Resources," *CBC News*, 20 February 2015, <http://www.cbc.ca/news/politics/csis-watchdog-agency-starved-of-staff-resources-1.2965276>.
28. A useful summary of Snowden's impact on Canada can be found in Michael Geist's blog, "Citizen Four and the Canadian Surveillance Story," 23 February 2015, <http://www.michaelgeist.ca/>.
29. *Supra* note 5.
30. *Proceedings of the Standing Senate Committee on National Security and Defence*, Issue 15: Evidence (30 April 2007). Semantic hair-splitting over distinctions between data and metadata bring to mind the notorious "Clinton defence" ("I did not have sex with that woman").
31. Office of the Information and Privacy Commissioner of Canada, *Metadata and Privacy: A Technical and Legal Overview*, October 2014, <https://www.priv.gc.ca/information/research-recherche/2014/md_201410_e.asp>.
32. British Columbia Civil Liberties Association, "Stop Illegal Spying — Case Details" <https://bccla.org/stop-illegal-spying/protect-our-privacy-case-details/>.

33. "Too much information going in…," *Globe and Mail*, Editorial 26 October 2013, <http://www.theglobeandmail.com/globe-debate/editorials/too-much-information-going-in/article15092678/>.
34. Greg Weston, "Spy agency CSE Needs MPs' Oversight ex-Director Says," *CBC News*, 7 October 2013, <http://www.cbc.ca/news/politics/spy-agency-csec-needs-mps-oversight-ex-director-says-1.1928983>.
35. Bill C-51, *The Anti-Terrorism Act*, 2d Sess, 41st Parl, 2015, C-51.
36. See for instance the open letter to parliamentarians from over 100 academics, mainly from law faculties across the country: "Open letter to Parliament: Amend C-51 or kill it," *National Post*, 27 February 2015, <http://news.nationalpost.com/full-comment/open-letter-to-parliament-amend-c-51-or-kill-it>. Disclosure: I am one of the signatories.
37. Jean Chrétien, Joe Clark, Paul Martin & John Turner, "A Close Eye on Security Makes Canadians Safer," *Globe and Mail*, 19 February 2015, <http://www.theglobeandmail.com/globe-debate/a-close-eye-on-security-makes-canadians-safer/article23069152/>.
38. Craig Forcese & Kent Roach, *Bill C-51 Backgrounder #2: The Canadian Security Intelligence Service's Proposed Power to "Reduce" Security Threats Through Conduct that May Violate the Law and Charter* (February 12, 2015), <http://ssrn.com/abstract=2564272> or <http://dx.doi.org/10.2139/ssrn.2564272>.
39. Daniel Therrien, "Without Big Changes Bill C-51 Means Big Data," *Globe and Mail*, 6 March 2015, <http://www.theglobeandmail.com/globe-debate/without-big-changes-bill-c-51-means-big-data/article23320329/>.
40. "Edward Snowden Says Canadian Spying Has Weakest Oversight in Western World," *CBC News*, 4 March 2015, <http://www.cbc.ca/news/canada/edward-snowden-says-canadian-spying-has-weakest-oversight-in-western-world-1.2981051>.
41. Mike Frost as told to Michel Gratton, *Spyworld: Inside the Canadian & American Intelligence Establishments* (Toronto: Doubleday, 1994); Andrew Mitrovica, *Covert Entry: Spies, Lies and Crimes Inside Canada's Secret Service* (Toronto: Random House Canada, 2002).