Bill C-51 Backgrounder # 3: Sharing Information and Lost Lessons from the Maher Arar Experience

Kent Roach[*] and Craig Forcese[**]

This is the third of a series of independent "backgrounder" documents that we shall author on Bill C-51, the Anti-terrorism Act 2015. All of these documents are archived at www.antiterrorlaw.ca.

Abstract

The proposed *Security of Canada Information Sharing Act* in Bill C-51 declares a legitimate government interests in sharing information about security threats. Yet after close textual review, we conclude that the proposed law is both excessive and unbalanced. Why do we reach such strong conclusions?

The Act will relax constraints on the flow of information about "activities that undermine the security of Canada". This is a new and astonishingly broad concept that is much more sweeping than any definition of security in Canadian national security law. In comes very close to a *carte blanche*, authorizing a "total information awareness" approach and a unitary view of governmental information holding and sharing. In that respect, we consider it a radical departure from conventional understandings of privacy.

The proposed legislation is unbalanced because it authorizes information sharing without meaningful enhanced review. While the bill pays lip-service to accountability, it does not incorporate an accountability regime matching its scope. Even as it erodes privacy, it fails to learn from the lessons of the Arar and Iaccobucci commissions of inquiry about the injustice that may stem from poorly governed information sharing. The claims in the government's backgrounder that the existing accountability institutions, including the Privacy Commissioner, are up to the task is not convincing to anyone familiar with the Arar report.

About this project

This is a working document. It is legal scholarship done in "real time" in a highly politicized environment, in which fundamental decisions about the shape of law are being made.

There will be typos and glitches. We shall continue to develop this paper and its counterparts on different aspects of Bill C-51, adding more discussion, references and footnoted sources. We also anticipate developing the ideas and conclusions we present. We welcome (and very much encourage and need) feedback, critiques,

---

[*] Professor of Law, University of Toronto

[**] Associate Professor of Law, University of Ottawa

suggestions and observations from other lawyers, legal scholars, security and privacy experts and other interested persons with expertise to contribute (whether practical, legal, scholarly). We are, in other words, calling for a "crowdsourced" response to Bill C-51, and in this paper, to its information sharing regime.

We add an additional word relevant to this, a document dealing with security information sharing. We are legal academics who have been researching and writing on issues of national security law (Canadian, international and comparative) for a sum total of 26 person years (between the two of us). We have never worked in a security service. Instead, one or both of has worked with (or been involved in) two commissions of inquiry examining the security services (the Arar and Air India inquiries), a number of national security cases in the courts and several other commissions of inquiry focusing on state wrongdoing, including in the criminal justice sector. We are, in other words, an occasional and minor part of the national security "accountability sector", to the extent that such a thing exists in Canada.

Our legal expertise informs our legal conclusions. Our accountability perspective and experience informs our comments on operational issues.

There will be those who disagree with us, especially in relation to our operational concerns. We invite debate and discussion. That is the very reason we are conducting this project. These issues are too important to be swept up in partisan political positioning and infighting, and the debate should be informed and acute.

Please send feedback to: cforcese@uottawa.ca and kent.roach@utoronto.ca

Table of Contents

Summary of Key Concerns

Information sharing is a necessary feature of 21st century whole-of-government approaches to security. It seems sensible, even logical. Many people will wonder why we should be concerned. For two principal reasons: privacy and injustice.

Privacy and the Right to be Left Alone

Privacy is, in our society, the right to be left alone by the state. It is guarded by rules limiting collection, search and seizure and also by rules about what government can do with the information in its possession. But more than anything else, it is guarded by practical anonymity – the fact that government is not allowed, or not able, to compile and then share a complete and detailed portrait of every person's entire life. Technology has eroded practical anonymity – "big data" processing enables incredibly detailed and potentially intrusive monitoring and scrutiny of people's behaviour. Law stands then as the remaining bulwark against the end of privacy.

Privacy laws shackle government. There is an argument for relaxing those constraints in response to real threats, and that is an earnest debate we should have.

But if the objective is antiterrorism, then a law that relaxes rules on information sharing should be about terrorism, and not overreach into a potentially endless and ever mutable range of "security" concerns. As we discuss below, such vast overbreadth is exactly what this proposed Act will achieve.

Forgetting the Lessons of Arar

But even if it were more reasonable in its scope, this bill fails to include proper safeguards. Section 3 states that the Act's purpose "is to encourage and facilitate the sharing of information among Government of Canada institutions in order to protect Canada against activities that undermine the security of Canada." In what we have called "Arar amnesia", there is nothing in the proposed Act about steps to ensure the reliability and (for the most part) relevance of the information that is shared.

We raise, here, the injustice implications of sweeping information sharing of intelligence with varying levels of reliability. Improperly shared information may result in rumours and innuendo being reconceived as fact, and used to justify action, sometimes of a very troubling sort.

Information sharing of this sort lay at the core of the Arar commission of inquiry. There, the RCMP's ill-considered provision to American authorities of raw information, along with sensationalist commentary on the putative affiliation with al-

Qaeda of Mr. Arar and his wife Monia Mazigh, was the likely cause of Arar's rendition to Syria, a state in which he was tortured.[1]

Information sharing was also the key feature of the subsequent Iacobucci inquiry, examining the mistreatment of Adbullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin. There, commissioner Iacobucci concluded that Canadian officials indirectly contributed to the maltreatment of these individuals in foreign custody when they shared information about the detainees (especially about suspected terrorist involvement).[2]

The Arar commission recognized (wisely) that precautions were necessary to avoid these injustices. Those conducting national security investigations should be extremely well trained, including on how to analyze information with accuracy, precision and a "sophisticated understanding of context".[3] Information sharing decisions should be centralized, and governed by clear policies on screening for reliability, relevance and accuracy.[4] Caveats limiting who can have access to the information and how it can be further transmitted must be attached to shared information.[5]

Most important, integrated information sharing must be matched and balanced with integrated independent and review by independent review bodies[6] able to self-initiate their own investigations to ensure reliability, relevance, compliance with Charter and privacy rights.

The government has failed to honour these recommendations in this bill.

The Charter restraints on information sharing have expanded considerably since the 2006 Arar report, but are only invoked (and not operationalized) in an unenforceable preamble of the proposed bill. The lack of practical attention to review and accountability in Bill C-51 means that Charter rights will be difficult to enforce. As the Arar Commission recognized, many victims of information sharing may not even know that they have been victims given the secrecy of the process. This is why the

---

1 Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Ottawa: Public Works and Government Services Canada, 2006) [Arar inquiry, Factual Report].

2 Government of Canada, Honourable Frank Iacobucci, Report, Internal Inquiry into the Actions of Canadian Officials in Relation Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin (Ottawa: Public Works and Government Services, 2008).

3 Arar inquiry, Factual Report, above note 1 at 365.

4 *Ibid* at 366.

5 *Ibid* at 366.

6 See the many recommendations of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities* (Ottawa: Public Works and Government Services Canada, 2006) [Arar inquiry, Policy Report]

Arar Commission stressed the need for self-initiated review by those who could see all the secret information.

In addition, the bill contains several provisions that run counter to lessons that should have been learned from the Arar saga. There is no safeguard designed to ensure reliability of information, and only rudimentary consideration of relevance. The robust immunity from civil liability for good faith disclosures in s.9 of the new Act combined with its authorization in s.6 for lawful disclosure of information (in accordance with the law) "to any person, for any purpose" runs the risk of repeating the Arar pattern of unfettered information sharing on a domestic stage and possibly internationally, minus the government's payment of compensation.

We focus next on the two key aspects of the Act: its wildly overbroad concept of security and the broad range of disclosure it will authorize.

A Vast and Unprecedented Concept of Security: The is not just (or even mostly) about terrorism

The twin concerns of privacy and injustice might be tempered by a carefully confined scope of information sharing. However, the proposed Act is built on a wildly overbroad concept of "activities that undermine the security of Canada". This is new concept in Canadian law. It means any activity "that undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada". This concept, defined in such an open ended manner in s.2 of the Act, amounts simply a mutable, "eye of the beholder", public interest authorization for information sharing.

This concept is much broader than even "threats to the security of Canada" as defined in s.2 of the CSIS Act, and the government has offered no convincing explanation of why the latter concept (which still governs the CSIS Act) is not adequate for information sharing purposes. Indeed, the new provision is broader than even the sweeping definition of national security labelled "prejudice to the safety or interest of the State" in Canada's official secrecy law.[7]

It is, quite simply, the broadest concept of security that we have ever seen codified into law in Canada.

In the absence of cogent explanations for why such sweeping breadth serves this bill's nominal preoccupation with security (and specifically, antiterrorism), we are forced to the conclusion that the government wishes to share information about sovereignists, Aboriginal and environmental activists who may engage in "unlawful" forms of protest that may "undermine" (an undefined term) Canada's "territorial integrity" or its "critical infrastructure" or even the Government's capabilities with respect to Canada's "economic or financial stability" (all concepts identified in in the proposed Act).

---

7 *Security of Information Act*, R.S.C., 1985, c. O-5.

The government has also captured activities "that take place in Canada and undermine the security of another state". Since this is not contained to activities that are surreptitious or deceptive or unlawful, it easily reaches activities by dissidents opposed to (potentially repressive) foreign regimes and could impact and chill political activities by diaspora groups in Canada.

The new and untested definition of activities that "undermine the sovereignty, security or territorial integrity of Canada" also averts to more old-fashioned and more expansive ideas of subversion than are found in the CSIS Act. Whereas subversion is indexed to violence in the 1984 CSIS Act, in the proposed Act the orbit of targeted activities includes "changing or unduly influencing a government in Canada", "by force or by unlawful means." A street protest done without permit is an "unlawful" protest. It is directed at "changing" or "unduly" (whatever that means) influencing a government, and thus falls within the ambit of this Act.

We take little comfort in the only limitation imposed on this breathtakingly broad definition of the government's security interests: namely that is does not reach "lawful advocacy, protest, dissent or artistic expression". The term "lawful" is an unimpressive constraint on government authority under the proposed Act, since technical non-compliance with any number of regulatory rules (including permits for a protest) are enough to make conduct "unlawful".

We also must conclude that the government has deliberately rejected the approach found in Bill C-36, the original 2001 *Antiterrorism Act*. That law codified the then-new concept of "terrorist activity" and extended its reach to serious interference or disruption of an essential service. However, it then excluded circumstances where the disruption stemmed from (even unlawful) protests and strikes, so long as they were not intended to cause death, bodily harm or endanger life or cause serious risk to health.

What the government can do in the name of "security"

This is a law about an "all of government" "total awareness" strategy. Section 5 is the confusing and opaque heart of the proposed Act. It authorizes disclosure from government agencies to other government agencies, "in respect of" activities that undermine the vast security concept named in the Act, "including in respect of their detection, identification, analysis, prevention, investigation or disruption". Although it incorporates existing legal restrictions on disclosure, we conclude that these are not amplified in the Act and not very robust in other acts, including the Privacy Act and security legislation.

We also express concerns that s.5 provides an confusing and unstable mix of references to the existing jurisdiction and legal authorities of 17 different institutions that can provide or receive information under Schedule III of the act and now overlays these with the extremely overbroad concept of "activities that undermine the security of Canada". This blurring of legal authorities is then made more concerning by reference to each of the 17 institutions being able to use the information in relation to activities that undermine the security of Canada "including

in respect of their detection, identification, analysis, prevention, investigation or disruption."

The 17 institutions include not simply the security services (CSIS, CSE and the RCMP) but also revenue, finance and border control agencies. Regulations unilaterally decided by the executive could add (or subtract) from the list. Only one review body, the Commissioner who reviews CSE, our signals intelligence agency, is on the list.

Although the unenforceable "principles" enumerated in the Act recognize the importance of respecting "caveats" controlling secondary distribution of shared information, s.6 effectively authorizes the breach of caveats by providing that once information is shared with one of 17 recipient institutions, it can then be further shared "to any person, for any purpose" so long as the sharing is not legally prohibited. Caveats are not law, and so disregard of them is not prohibited.

In sum, we confront a proliferation of varying rules and strictures on disclosure, now seemingly bent in service of a vast concept of "undermining the security of Canada". We have considerable difficult imagining how all this will be governed in a sensible manner.

What about accountability

The secrecy of information sharing means, as the Arar Commission recognized, that legal restrictions on information sharing (including growing and robust Charter restrictions), will be under-enforced in the absence of integrated and self-initiated review. This is not included in the bill.

The government's backgrounder cites the Auditor General and the Privacy Commissioner as "whole of government" reviewers. But neither the Auditor General nor the Privacy Commissioner has a mandate to ensure that information sharing is reliable, relevant and in accordance with all legal restrictions of all sorts.

The Privacy Commissioner will make his views known at the appropriate moment. We note, however, the Privacy Commissioner's preliminary response to bill C-51 appears generally in accord with our concerns.[8] Likewise, former interim Privacy Commissioner Chantal Bernier has voiced concerns about the "increase[d] surveillance powers without increased oversight structure".[9]

In a 2014 report, the Privacy Commissioner observed that: "the *Privacy Act* remains essentially unrevised since 1983. Under the legislation, there are no provisions for joint audits or investigations with other like bodies, even in an era where

---

[8] Statement from the Privacy Commissioner of Canada following the tabling of Bill C-51 (Jan 30, 2015), available at https://www.priv.gc.ca/media/nr-c/2015/s-d_150130_e.asp.

[9] Chantal Bernier, "Too far, too fast?", iPolitics (Feb 12, 2015), online: http://www.ipolitics.ca/2015/02/12/chantal-bernier-on-the-terror-bill-too-far-too-fast/

information-sharing has increased greatly."[10] The report recommended that the *Privacy Act* be amended to allow the Commissioner to have access to the Federal Court in relation to collection and disclosure of information and that it be empowered to work jointly with other review bodies. There are no such amendments in Bill C-51 – the government has chosen to accelerate information sharing while leaving review bodies mired in shortcomings that make it difficult for them to perform their functions even at present.

The Auditor General focuses on financial and management effectiveness audits. The Auditor General has performed important performance audits in the national security agency but these are sporadic and can require up to 18 months to complete. The Arar Commission considered its powers and those of other review bodies but still found them to be inadequate in light of the demands of review of secret national security activities and in particular information-sharing.[11]

Meanwhile, it will be close to impossible to challenge any government conduct under this Act in court. The Arar Commission found that reliance cannot be placed on judicial enforcement with respect to many national security activities, including information sharing, because secrecy means "affected persons may never know that they have been the subject of a national security investigation".[12]

We know from past experience that a person flagged as a person of interest in one government database may remain there for a long time, before a matter is resolved and an entry deleted. Now that "flagging" may flow through all of government, difficult to monitor and virtually impossible to correct. Such "watch-listed" persons may wonder why they encounter regular difficulties in dealing with so many branches of the state, even as they try to correct misinformation originating from a single source.

Improperly controlled and supervised information sharing that includes no safeguards on relevance and reliability is the equivalent of a privacy virus, one that will be very difficult to remedy. It also has adverse implications for robust protest and democratic dissent, and will likely affect some groups and communities much more than others.

---

[10] Office of the Privacy Commissioner *Special Report to Parliament on Checks and Controls: Reinforcing Privacy Protection and Oversight for the Canadian Intelligence Community in an Era of Cyber-Surveillance*, January 28, 2014 at https://www.priv.gc.ca/information/sr-rs/201314/sr_cic_e.asp

[11] Arar Inquiry, Policy Report, above note 6 at 291-4

[12] *Ibid* at 491.

Introduction

In this paper, we analyze in detail the proposed *Security of Canada Information Sharing Act* (the Act or information sharing Act). Our analysis proceeds in a layered fashion. In the section that follows, we identify themes that animate our critique and reflect our chief concerns, tied to specific provisions in the Act.

For readers who wish to probe the fine details, in Part II, we examine and annotate the chief components of the Act in greater detail, and in the order they appear, beginning with the preamble. Our focus here is on trying to understand what the various provisions mean, and how they relate to one another.

Part I: An Overview of the Act's Architecture and Effect

The 10 page Act proposed at the start of Bill C-51 is one of the most important, but most opaque and troubling, parts of the bill. It clearly aims to achieve a "whole-of-government" information sharing in relation to a wide range of concerns. These concerns stray well away from conventional national security preoccupations, as they have commonly been defined in Canadian law and practice.

A. The Objective of Total Information Awareness

Total information awareness is a controversial concept – it is what senior Department of Justice lawyer Stanley Cohen identified and criticized as "a unitary view of government information holding." Writing in 2005, he observed:

> A belief exist…that the government should consider legislative change that will allow it to view all data collected by institutions as belonging to one party - the government. Government institutions would merely be custodians of what would essentially amount to a centralized pool of personal information. Needless to say, this unitary view of government information-holding is highly controversial and has never been official endorsed. By this view, the government would reserve the right to share information horizontally for greater protection and security when it is in the public interest to do so.[13]

Whatever the merits of total information awareness for anti-terrorism and *bona fide* national security concerns, it becomes acutely troubling when extended to other conduct in a democratic society.

[13] Stanley A Cohen *Privacy, Crime and Terror Legal Rights and Security in a Time of Peril* (Toronto: LexisNexis, 2005)at 104

B. The Breadth and Scope of the New Act

The Act would allow those within the government of Canada to share information about the new and disturbing concept of "activities that undermine the security of Canada". It is difficult to overstate how broad this new definition is, even as contrasted against existing national security definitions in s.2 of the CSIS Act[14] and s.3 of the *Security of Information Act*.[15]

1. The "Headline" Concept

The Act defines the concept as follows: *any* activity, including any of the activities then enumerated as examples, "if it undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada". "People of Canada" means "people in Canada" or *any* citizen or permanent resident who is *outside* Canada. Put another way, the definition reaches any activity that "undermines" the lives or security of any single Canadian anywhere in the world. There is no definition of "undermine".

2. Enumerated Examples

The Act lists examples of this threat concept – and these are mere examples since the Act is not confined to them.

"Terrorism" is identified as one. Even there, the choice was made to use the undefined term "terrorism"[16] as opposed to the better understood, codified and still very broad concept of "terrorist activity", found in the Criminal Code. Other items on the list of examples of matters falling within the new definition are: "interference with critical infrastructure"[17] and "an activity that takes place in Canada and undermines the security of another state."[18]

The new definition includes examples of conduct that broaden greatly established (but still controversial) concepts of subversion. The notion of subversion found in s.2 of the CSIS Act focuses on violence and "covert unlawful acts" directed at destroying or overthrowing the constitutionally established system of government in Canada. The related concept of "sedition" in the Criminal Code also focuses on unlawful use of force to accomplish governmental change in Canada.[19]

---

[14] *Canadian Security Intelligence Service Act*, R.S.C., 1985, c. C-23

[15] *Security of Information Act*, R.S.C., 1985, c. O-5.

[16] *Security of Canada Information Sharing Act*, s. 2(d), being Part I of Bill C-51, the Anti-Terrorism Act, 2015

[17] *Ibid*, s.2(f)

[18] *Ibid*, s. 2(i)

[19] *Criminal Code*, s.59.

The proposed Act, by comparison, reaches the incredibly broad concept of "changing or unduly influencing a government in Canada by force *or* unlawful means."[20]

The only exemption in s.2 is for "lawful advocacy, protest, dissent and artistic expression".

3. The Limited Exemption for "Lawful" Protest

It is important to focus on this exemption for "lawful advocacy, protest, dissent and artistic expression." As is evident, everything hinges on the concept of "lawful". This is a very weak limitation on the scope of the Act. "Unlawful" conduct does, of course, include blockades. It also reaches workplace strikes inconsistent with labour law and street protests lacking the proper regulatory permits. Put another way, "unlawful" does not mean criminal. It just means without lawful authority.

Once labour, Aboriginal or environmental protesters break one law -- including a municipal by-law -- they fall outside the limited safeguards in the new Act. They are subject to security information sharing involving, at present (the number could increase) 17 different federal institutions including revenue, finance, health as well as CSIS, borders service, the RCMP and the CSE (Communications Security Establishment).

C. The Powers of the New Act

1. Disclosure

In its key operative provision, section 5 of the Act contemplates that a government institution may (unless other laws prohibit from doing so) disclose information to another institution in relation to "activities that undermine the security of Canada", including "in respect of their detection, identification, analysis, prevention, investigation or disruption".

The reference to "prevention" and "disruption" is notable, and its inclusion may undermine whatever limited checks the reference to "lawful" protest noted above provides. If an agency charged with "prevention" and "disruption" has reason to believe that a street protest may proceed in violation of municipal by-laws or that some other unlawful event might occur during the protest, this may be enough to trigger the information-sharing regime under the Act.

2. And More Disclosure

The extent of the contemplated information sharing is also reflected in Schedule 3, which lists 17 different government institutions. This list could be made longer or shorter by regulation, made unilaterally by the federal Cabinet.

---

[20] *Security of Canada Information Sharing Act*, s.2 (b) (emphasis added).

But information sharing is not limited to the scheduled institutions. Once it has been shared, s.6 of the Act would allow heads of institutions or their delegates to "in accordance with law…us[e] that information, or further disclos[e] it to any person, for any purpose."

"Any person, for any purpose" is about as expansive an expression as any Act might craft. It seems to allow the disclosure of information to the private sector and foreign governments so long as the disclosure is otherwise "in accordance with law". This law is not, in other words, strictly about internal, Government of Canada information sharing.

The repeated reference to disclosure being consistent with existing law gives us only modest comfort. That existing law is itself fairly rudimentary. There is no specialized law that *per se* regulates international information sharing. And the laws that reach information sharing in general, such as the *Privacy Act*, are riddled with exceptions and limitations to their reach. Put another way, a lot of information will now be moving in a relatively unconstrained manner within government, and potentially across borders.

3. Limited Internal Checks and Balances

The Act contains little in the way of built-in checks and balances on information sharing. As noted, nothing in the Act refers to the principle that information sharing should be guided by the reliability of the information -- something that the Arar Commission stressed.[21]

A non-enforceable principle found in s.4 state that "respect for caveats" and "originator control over shared information is consistent with effective and responsible information sharing". "Originator control" is a principle in information sharing practices that puts control over the subsequent use and distribution of shared information in the hands of the agency from which it comes. "Caveats" are an express (or implied) proviso attached to the shared information underscoring the existence of originator control, and sometimes superimposing other expectations on how the shared information is to be used.

Originator control and caveats are enforced, if at all, by the expectation of reciprocity: if violated, future information sharing may be imperiled. The Act does not enhance this (sometimes underwhelming) safeguard. It provides no enhanced means to ensure independent review and auditing of the enhanced information sharing it will enable. This means that, as in the Arar affair, a failure to place caveats

[21] Recommendation 8 was "The RCMP should ensure that, whenever it provides information to other departments and agencies, whether foreign and domestic, it does so in accordance with clearly established policies respecting screening for relevance, reliability and accuracy and with relevant laws respecting personal information and human rights." Arar inquiry, Factual Report, above note 1 at 334. See also 18,104,110, 120, 326, 331-2 for other discussions of the importance of the relevance and reliability of share information.

or restrictions on subsequent disclosure may not be detected or remedied, except by accident.

Moreover, s.6 of the Act seems implicitly to authorize breach of caveats by authorizing additional disclosure "to any person, for any person". Disclosure under s.6 must be "in accordance with law" but caveats do not generally have the force of law. They are created and hopefully respected by the agencies that engage in information sharing, and nothing more.

D. Implications

All told, the definition of "activities that undermine the security of Canada" coupled with the instructions in section 5 amount to sweeping and concerning new statutory powers that blur the existing jurisdiction of 17 different institutions.

We have specific "machinery of government and legal" concerns, operational security concerns and democratic concerns.

1. Machinery of Government and Legal Concerns

How will this all work? We are left unclear about exactly what is being authorized here, and what it will mean in practice. For instance, we have concerns that it could have the practical, trickle down effect of enlarging the *de facto* jurisdiction of 17 agencies ranging for CSIS, CSEC and the RCMP to Health, Transport, the Canadian Border Services Agency, the Canadian Revenue Agency or any other agency listed in Schedule III. The Act does provide that information may only flow where it is "relevant to the recipient institution's jurisdiction or responsibilities". In practice, what safeguards will be put in place to ensure that inbound information does not actually exceed the recipient's remit? "Jurisdiction and responsibilities" is pliable language, especially where there is no serious prospect of independent outside review. We think it likely that these agencies will be in receipt of information that they could not themselves collect.

The Act says disclosure is "subject to" any other Act or regulations restricting disclosure. We are not persuaded that this is as robust a constraint as might be hoped. But more than this, of course, constitutional rules apply. It is not clear to us that the host of persons empowered to share will be attuned to these constitutional expectations.

For instance, information sharing may not be employed by state agencies to circumvent constitutional privacy protections. Law enforcement agencies, for example, may not avoid constitutional search and seizure obligations by receiving otherwise protected information from administrative or other bodies not subject to the same constitutional strictures.[22] Where law enforcement agencies propose

[22] See, e.g., *R. v. Colarusso*, [1994] 1 S.C.R. 20 at para. 93 (rejecting an approach where "property is seized by one state agent for a purpose for which the prerequisites for search may not be as demanding, and another state agent, one forming part of the law enforcement apparatus of the state,

obtaining private information from other bodies that is protected by a reasonable expectation of privacy, warrants must be obtained, even in circumstances where disclosure of personal information is permissible under the *Privacy Act*.[23].

Likewise, information collected by warrant retains constitutional protections, and if is shared without being governed by a clear law, with reasonable safeguards and in a reasonable fashion, that behaviour too is unconstitutional.[24]

We do not expect government to disregard the law. We do expect that a large, vast new information sharing enterprise done without any serious prospect of independent review or court oversight will make mistakes. In the rare cases where the information sharing results in a prosecutions, these mistakes may be uncovered and result in a constitutional remedy such as the exclusion of evidence. In our view, it is better to have robust review of all information sharing rather than to rely on such infrequent and drastic remedies.

2. Operational Concerns

There is presently an acute concern in security discussions that we are now overloaded with too much information and too little analytical capacity and rigour. If so, the new Act risks more of the disease of agencies drowning in data. It opens the possibility that the 17 institutions that can share information under the new Act may simply swamp themselves in data and prove unable to separate the truly dangerous threats from "threats" that are simply annoying and irritating.

The data that is shared under the act may include such a range of information about diverse matters such as domestic "subversion" by separatist, Aboriginal and environmental groups, to concerns about the security of other states, to harm to infrastructure. We have concerns, augmented by what is being learned from the Snowden leaks about the collection of "big data", that officials under this proposed Act may be unable to see the most immediate dangers of terrorism in the tidal wave of information that will be shared under this Act.

History is littered with intelligence failures, including the failures to appreciated fairly specific intelligence to prevent the 9/11 events, the Air India bombing and possibly the Oct 22, 2014 attack on Parliament. Recent events in Europe and Australia suggest that the perpetrators of terrorism are often known to authorities, but their conduct not predicted. If we are unable to process warning signals properly

---

is permitted to claim the fruits of the search (the resulting information) for use for law enforcement purposes without regard to the rightly stringent prerequisites of searches for those purposes"). *R. v. Cole*, 2012 SCC 53, at para. 69 ("Where a lower constitutional standard is applicable in an administrative context, as in this case, the police cannot invoke that standard to evade the prior judicial authorization that is normally required for searches or seizures in the context of criminal investigations"). See also discussion in Cohen, above note 13 at 98, 120 and 137.

[23] *Ibid*. at 120.

[24] *Wakeling v. United States*, 2014 SCC 72

even in relation to terrorism, what are the implications of data sharing that reaches the vast universe of matters labelled a security risk in the new Act?

If everything is a security matter (as it appears to be under this Act), nothing is. The advent of big data aggravates this problem. In sum, we fear that the information sharing Act may make it more, not less difficult, to single out information and intelligence that might stop an act of terrorism.

We admit we may be wrong. The security professionals may be able to separate the wheat from the chaff. But we are confident as lawyers in concluding that the proposed information sharing Act will include a lot of chaff.

If the threat from Al Qaeda/ISIL-inspired terrorism is significant, we should not be enacting overbroad legislation that will throw terrorist together with unlawful (e.g., without the right permit) protests or those who threaten the security of another country in a non-violent and non-deceptive manner.

3. Democratic Concerns

a. Overbreath and Democratic Dissent

The Act plainly reaches information sharing in relation to conduct that is commonplace in a democracy. The Act easily encompasses, for example, any Quebec sovereignist, and Aboriginal and environment or diaspora movement that does (or even may) engage in conduct that does not strictly conform to the law – including regulatory rules or municipal by-laws.

More expression and more protests utterly unconnected to violence will presumptively be subject to an "all-of-government" "total awareness"-like policy. This may be sensible for a much reduced subset of threats encompassed by the Act's new "threat" definition, but it could also chill other, much less pernicious activities.

We do not discount the chilling impact information sharing and "total government awareness" may have on expressions of dissent. Nor are we persuaded that mere information sharing is benign. As we have underscored above, the experience with commissions of inquiry in the past decade shows that information sharing can be the causal origin of significant harm.

b. Review and Accountability

The proposed information sharing Act raises key questions of review and accountability. The only explicit reference to accountability is in a non-enforceable preamble.

There are no provisions for judicial oversight, as there is with CSIS warrants.

The government's backgrounder on the bill expresses confidence that the review functions of the Privacy Commissioner and the Auditor General "will help maintain

the appropriate balance between protecting the privacy of citizens and ensuring national security".[25] It fails to mention other concerns identified by the Arar Commission about the need for independent reviews agencies able to "self-initiate" investigations to ensure the legality, reliability and propriety of information sharing, and to coordinate with one another.[26]

Indeed the Arar Commission found that while the Auditor General has done valuable work on national security "it does not have the expertise to review RCMP national security activities [there at issue] to ensure their legality and propriety" and the Privacy Commissioner had admitted that it did not have sufficient resources to adequately provide accountability.[27] As we have noted above, in 2014, the Privacy Commissioner's office underscored continued difficulties in reviewing national security matters, and called for wholescale reform.[28] This reform has not come to pass.

Meanwhile, the Privacy Commissioner's remit extends only to "personal information". While that concept is broadly defined in the *Privacy Act* as "information about an identifiable individual", it may not reach all the information that might be at issue under the new sharing regime.

Consider the implications of whole of government information sharing and the "mosaic effect". Government agencies may each individually share pieces of information that themselves do not include information about an "identifiable individual". In this respect, the government might argue that the sharing is ungoverned by the *Privacy Act*, and unreviewable by the Privacy Commissioner. However, once assembled through "big data" processing, the information the information may be combined to present a mosaic that does implicate serious privacy concerns. Bits of information that themselves are not attached to a person may be assembled and interpolated to say a lot about a now imputable individual's behaviour. The government might urge that the point of assembly is where the *Privacy Act* attaches, and not before. Such an approach would greatly limit the ability of the Privacy Commissioner to investigate and review the whole "life cycle" of information sharing within government.

The government backgrounder on the new Act notes that there are review bodies for CSIS, CSEC and the RCMP, but this disregards the Arar Commission's finding that review bodies could not adequately review information sharing between institutions when the review bodies' jurisdiction remained stovepiped or siloed by agency.[29]

---

[25] Government of Canada, Backgrounder Security of Information Sharing Act (Jan 30, 2015), online: http://news.gc.ca/web/article-en.do?nid=926879.

[26] See note 6 above.

[27] Arar inquiry, Policy report, above note 6 at 286, noting that while the Privacy Commissioner reviews some national security activities, it "does not have the resources to thoroughly audit, review or investigate all national security actors".

[28] See note 10 above.

[29] Arar inquiry, Policy report, above note 6 at 483-496.

It must always be remembered that secrecy will be claimed over most national security information sharing. It was for this reason that the Arar Commission recommended in Recommendation 9 that the mandate of SIRC be expanded to include Canadian Border Services, Citizenship and Immigration, Transport Canada, FINTRAC and DFAIT (all included in the 17 recipient institutions under the proposed act) and that "statutory gateways" be created to allow the review bodies to share information and conduct joint investigations.[30]

"All-of-government" total information awareness should be matched by all of government total review and accountability. Such a system does not exist in Canada. For instance, the Arar Commission noted the absence of review of border operations and diplomatic or consular relations. The 2010 Afghan detainee affair also demonstrated the limits of review with respect to national defence activities.

What this Act does is break down barriers between government agencies while keeping review bodies carefully corralled to a narrow subset of agencies.

Lest these concerns of enhanced review be dismissed as "needless red tape"[31], we want to be clear that modernized review could involve reducing the number of institutions that conduct review, but giving the remaining reviewers both adequate resources and whole of government mandates to conduct review.

We at present favour the creation of a "super SIRC" that like the Inspector General in Australia could be given a mandate over all national security activities in government, including information sharing. We will return to this question of institutional design in another paper.

Part II: Detailed Review of Elements of the Act

We now drill down further into the details of the Act.

A. The Preamble

The information sharing Act, alone of the new measures in the omnibus Bill C-51, features a preamble. Preambles are an uncommon practice in Canadian law making. There are a number of reasons why the government might include a preamble, including political positioning. Preambles have been included in criminal law bills in

---

30 *Ibid*, Recommendations 11 and 12

31 David Pugliese "Government knows best, says Conservative MP, no need for more oversight on spy and security agencies" Ottawa Citizen Feb. 1, 2015 Aaron Wherry "The Heart of our Democracy in a Time of Terror" Macleans Feb 5, 2015 at http://www.macleans.ca/politics/the-heart-of-our-democracy-in-time-terror/

the past when bills have responded forcefully to Charter decisions rendered by the Supreme Court.

Preambles are found in other national security legislation – not least the 1988 *Emergencies Act*.

Preambles to legislation are an expression of "legislative intent".[32] They seek to outline the government's objective for legislation, something that might influence how courts interpret the substantive provisions in the statute. These political statements may also become material in the event of a Charter challenge (and a subsequent effort to defend the law on s.1 grounds as reasonable in a free and democratic society). The preamble in the proposed new Act no exception. The first 6 of 8 paragraphs of the preamble take this approach. We examine those aspects of the preamble that gave us pause.

1. Threats to Canadian Security

The preamble asserts that "the people of Canada" (defined as people in Canada and citizens and permanent residents abroad) "are entitled to live free from threats to their lives and their security." The sentiment is difficult to dispute, although the objective seems to contemplate an unrealistic "zero threat" environment.

The preamble also asserts "there is no more fundamental role for a government than protecting its country and its people." This seems to link both a defence of Canada rationale ("protect our country") and a crime rationale ("protect our people") to the Act's objectives (and therefore, its broad understanding of national security). We are struck by the reference to "no more fundamental", and note that the government has advanced in other contexts – including immigration security certificate court challenges -- the argument that security is primordial and trumps or constrains rights.[33] The position adopted by the courts is that the concepts of security and rights are to be reconciled and balanced.[34]

We are concerned that the national defence and crime protections rationales have been muddled in some of the political posturing on this bill, in a manner that detracts from public understanding and misstates the issues at stake. We shall address this issue in a subsequent paper.

We are also struck by how less nuanced this preamble is compared to the equivalent in the *Emergencies Act*, an instrument consciously designed to allow for aggressive government responses to the most extreme emergencies. The latter statute says "the safety and security of the individual, the protection of the values of the body politic and the preservation of the sovereignty, security and territorial integrity of the state

---

[32] Ruth Sullivan, *Statutory Interpretation* (Irwin Law, 2007 2d ed) at 12 et seq.

[33] Janice Tibbets, "Judges question national security as a 'core value'", *Ottawa Citizen* (15 June 2006).

[34] *Application under s. 83.28 of the Criminal Code (Re)*, 2004 SCC 42 at para. 5 et seq.

are fundamental obligations of government". It does not suggest that this protection is the *most* fundamental role.

2. Threats to the Security of Other States

The preamble states that Canada "is not to be used as a conduit for the carrying out of activities that threaten the security of another state". This is operationalized in s.2(i) of the Act which defines activities that undermine Canadian security to include "an activity that takes place in Canada and undermines the security of another state." There is no definition of security of another state, and so the language clearly encompasses repressive states (including, for example, Syria). As we discuss in more detail below, this broad language goes beyond the closest equivalent found in the CSIS Act.

3. Whole-of-Government Approach to Security

The preamble notes that protecting Canadian security "often transcends the mandate and capability of any one Government of Canada institution." This recognizes, sensibly in our view, the need for a "whole-of-government" approach to security in the 21st century. It begs, however, the question of whether independent review of that information sharing is also conducted in a "whole of government" manner.

4. Unenforceable Reference to the Charter and Privacy

The preamble states that information should be "shared in a manner that is consistent with the Canadian Charter of Rights and Freedoms and the protection of privacy." This recognizes that information sharing implicates both ss.7 and 8 of the Charter and it may also engage s.15 of the Charter if discriminatory stereotyping is used.

The problem is the Act then does nothing to ensure proactively that these rights will be protected. We repeat: the Arar Commission found that reliance cannot be placed on judicial enforcement with respect to many national security activities, including information sharing because of secrecy, and the fact that people simply will not know of government wrongdoing. Even if they know that information has been shared, they will face the costs of going to court and resisting the government's secrecy claims in such litigation.

5. Unenforceable Reference to Accountability

The last paragraph of the preamble asserts that federal "institutions are accountable for the effective and responsible sharing of information." This implicitly contradicts the findings of the Arar Commission that the *status quo* with respect to review of national security activities was not adequate, and enhanced independent review was essential. The Commission warned that there was a need to modernize the review of national security activities in 2006. The nine years since that report has been issued have only increased the need to modernize review.

B. Section 2: An Overbroad and New Definition of an "Activity that undermines the security of Canada"

1. Past Analogues

Canada has many legislated national security definitions. The best known is contained in s.2 of the CSIS Act, as is discussed in length in our separate backgrounder on Bill C-51's amendments to the CSIS Act. This CSIS definition emerged in part though the work of the McDonald Commission into RCMP wrongdoing in the 1970s. It defines threats to the security of Canada as follows:

> (*a*) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage,
>
> (*b*) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person,
>
> (*c*) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against per- sons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state, and
>
> (*d*) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada,
>
> but does not include lawful advocacy, protest or dissent, unless carried on in conjunction with any of the activities referred to in paragraphs (*a*) to (*d*).

As we discuss in our backgrounder #2 on CSIS, this definition is broad and many of its terms are uncertain, and has been criticized for that very reason, including by SIRC.

Nevertheless, this definition is an exercise in restraint compared to that deployed for the new Act. Likewise, the new Act's national security concept far exceeds the more closed-ended reach of "prejudicial to the safety or interests of the State", a concept at the heart of Canada's official secrets statute.[35]

2. The New Definition

[35] *Security of Information Act*, above note 15, s.3.

The government could easily have used these more restrained definitions in the information-sharing Act. It chose not to, presumably consciously and for reasons we fail to understand.

Instead, the new Act is indexed to an "activity that undermines the security of Canada". The accompany definition then reads:

> any activity, including any of the following activities, if it undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada:
>
> > (a) interference with the capability of the Government of Canada in relation to intelligence, defence, border operations, public safety, the administration of justice, diplomatic or consular relations, or the economic or financial stability of Canada;
> >
> > (b) changing or unduly influencing a government in Canada by force or unlawful means;
> >
> > (c) espionage, sabotage or covert foreign-influenced activities;
> >
> > (d) terrorism;
> >
> > (e) proliferation of nuclear, chemical, radiological or biological weapons;
> >
> > (f) interference with critical infrastructure;
> >
> > (g) interference with the global information infrastructure, as defined in section 273.61 of the National Defence Act; [that provision reads: "*"global information infrastructure"* includes electromagnetic emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those emissions, systems or networks."]
> >
> > (h) an activity that causes serious harm to a person or their property because of that person's association with Canada; and
> >
> > (i) an activity that takes place in Canada and undermines the security of another state.
>
> For greater certainty, it does not include lawful advocacy, protest, dissent and artistic expression.

This definition will allow government to share information about a staggering range of very loosely defined "threats" to Canada.

The "headline" part of the definition is anything that "undermines the sovereignty, security or territorial integrity of Canada or the lives or the security of the people of Canada". This concept is the only outer limit on the new powers to share information. The more detailed items listed in the definition are examples – they do not represent the sum total of everything that can fall within the "headline".

We review the "headline's" elements.

a. Threats to the Sovereignty or Territorial Integrity of Canada

A major factor leading to the creation of CSIS and the abolition of the RCMP Security Service was the latter inability to distinguish democratic from violent aspects of the sovereignist movement in Quebec.

The CSIS definition of "threats to the security of Canada" learned from this experience and inserted language tying security threats to violence. As we discuss in our backgrounder #2 on CSIS, the definition is imperfect and especially troubling when used as the index for CSIS's new powers in bill C-51. But whatever the shortcomings of the CSIS Act, they pale in comparison to the new definition.

That new definition will reach those in Quebec, in Aboriginal movements or elsewhere who would "undermine" Canada's sovereignty and territorial integrity by agitating in favour of diminished federal or provincial control over territory within Canada. Its focus on territorial integrity is in tension to the Supreme Court's recognition that secession from Canada has been a legitimate feature of political debate in Canada.[36]

It must be underscored again that the list that follows the "headline" is merely illustrative. Whatever constraint found in those listed items need not be applied to the open ended language of the "headline". The only limiter on the headline is the proviso limiting the definition's application to "lawful advocacy, protest, dissent and artistic expression"

An unlawful strike or unlawful protest in favour of Quebec separatism (that is, one down without the proper municipal permit) would, therefore, be included, as might unlawful aspects of the Idle No More movement such as blockades.

If we are correct, information about separatist and Aboriginal groups could be shared under this act. Indeed, to the extent an agency is tasked with preventing or disrupting "threats" as defined in the statute, information sharing may be preemptive, responding to feared and not yet manifest "unlawful" advocacy or protest.

The government will likely protest that the Act does nothing more than ease information sharing about these protests activities. They would be right. But it does so in a manner that, by definition, singles out these activities as "an activity that

---

[36] *Reference re Secession of Quebec* [1998] 2 S.C.R. 217.

undermines the security of Canada". We have already discussed the privacy and injustice concerns with relaxed information sharing. Here, we simply point out that branding dissent as "undermining" security bears a stigma that has democratic repercussions.

b. "Activities that undermine the security of Canada or the lives or the security of people of Canada"

The "headline" definition of threats also invokes "security of Canada" and "lives or security of people of Canada". "Security of Canada" is not defined and presumably means something more than threats to the lives or security of Canadians. It may be read in reference to the broad definition of security in other parts of the Act referring to matters such as "the economic or financial stability of Canada" and interference with critical and global information infrastructure. Or it may be read with an eye to the concept of "threats to the security of Canada" in the CSIS Act.

But whatever it means, the reference to "lives or security of people of Canada" is expansive. "People of Canada" means "people in Canada" or *any* citizen or permanent resident who is *outside* Canada. Put another way, the definition reaches any activity that "undermines" the life or security of any single Canadian anywhere in the world.

As nowhere in the Act is there any definition of "undermine", the range of things that might connect to the life or security of every, single Canadian, no matter where, is virtually unlimited.

c. The Nine Categories of Activity that Undermine the Security of Canada

The definition then includes an illustrative list of things meeting the "headline" definition. As noted, these are simply examples, although as a matter of statutory interpretation, these examples will colour how the "headline" definition is construed, assuming it was ever possible to bring government action under the Act to court.

a) Interference with Governmental Capabilities

The first of nine is one of the broadest categories. It refers to any activity that interferes with the capability of Canada in relation to

1) intelligence
2) defence
3) border operations
4) public safety
5) the administration of justice
6) diplomatic or consular relations
7) economic or financial stability of Canada

In our view, the reference to "public safety" is much too broad and would allow the Act to be used for the sharing of information about many forms of non-political crime.

Similarly the reference to "economic or financial stability of Canada" is overbroad and both of these should be deleted if there is to be any credibility to the government's claims that the act relates to genuine issues of Canada security.

Our concerns stem from both rights and security: two much information both affects Charter freedoms and can drown the government in data that is not essential to maintain our safety.

The other aspects of the list in paragraph (a) of the definition are broad, but at least refer to matters that truly constitute national security concerns.

b) changing or unduly influencing a government in Canada in Canada by force or unlawful means

This is a new and expanded approach to subversion that is broader than that found in s.2(d) of the definition of threats to the security of Canada in the CSIS Act. The CSIS provision refers to "activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada." Whereas unlawful acts must be covert or violent to fall under CSIS's intelligence mandate, they only need to involve "force" *or* "unlawful means" to fall under this provision in the new Act.

We note that "sedition" in s. 59 of the Criminal Code also focuses on unlawful use of force to accomplish governmental change in Canada. Sedition is an old concept: the leading case where the Supreme Court read down its broad statutory language was decided in 1951.[37]

We are underscore that in both sedition and the CSIS mandate the requirement is for force *and* unlawfulness. In the new Act, the focus is on force *or* unlawfulness.

The risk is a mismatch between, e.g., what CSIS collects and a broader range of information it could receive from other government departments under the new Act. We confess a concern that the result may be a *de facto*, creeping expansion of CSIS's situational awareness and, potentially, a temptation to test the bounds of its actual mandate.

A subversion mandate tied to "force" *and* "unlawful means" is an early 20th century concept: it has echoes of a pre-Charter society where unions and other protest groups were treated as unlawful.

We see no reason why the government has resuscitated overbroad and old-fashioned concepts of subversion for the purpose of information sharing.

---

[37] *R. v. Boucher*, [1951] S.C.R. 295.

Our concern is made more acute by use of the word "influence". This is an incredibly broad concept – every protest seeks to influence, after all.

Use of this sort of language has drawn much criticism in the UK's Terrorism Act, 2000. For this reason and others, many anti-terrorism laws (including Canada's) use the more restrictive concepts of "intimidation" or "compel".

A focus on unlawful activity that uses force in order to "intimate" or "compel" a government would be a much more reasonable approach in a democracy.

c) espionage, sabotage or covert foreign-influenced activities

This example is relatively unobjectionable but the concept of sabotage should more clearly be related to the sabotage offence under s.52 of the Criminal Code.

d) terrorism

We are puzzled by use of this term and wonder how considered it is. The term is not defined, and it is different from the Criminal Code's concept of "terrorist activity".

It is, however, a term that has been construed in the caselaw. The Supreme Court interpreted "terrorism" in *Suresh v. Canada,*[38] an immigration case. "Terrorism", for the Court, is intentionally causing death or bodily harm to civilians outside of armed conflict.

This definition is in fact, substantially narrower than the definition of terrorist activity in s.83.01 of the Criminal Code. Has the government intentionally restrained itself to a narrower concept of terrorism? If so, this might be a good idea, but it opens up a disjunction between the mandate of the RCMP and other police forces which are linked to enforcing offences that incorporate the "terrorist activity" concept, and the potentially narrower meaning of "terrorism" (if that term is construed as it was in *Suresh*)

We appreciate that the broad "headline" definition preceding the examples would encompass the full range "terrorist activity", making a mockery of any restraint in the examples (real or accidental) should "terrorism" continue to be interpreted as a more restrictive concept than "terrorist activity". But we are perplexed by this obvious definitional uncertainty. Why draft this law in a manner that leaves Canadians and government officials guessing about what is meant by terrorism?

e) proliferation of nuclear, chemical, radiological or biological weapons

This is unobjectionable and reflects Canada's international security obligations.

f) interference with critical infrastructure

[38] [2002] 1 S.C.R. 3.

There is no definition of this phrase. It obviously includes pipelines and hydro transmission towers, even in remote areas, as well as important cyber systems. It could reach blockades of railways and roadways.

We note that it does not speak of "attacks" or "destruction" or "damage". Instead, it refers to "interference", and not even "serious" interference.

In the result, this concept is broader than the equivalent infrastructure concept in the Criminal Code's definition of "terrorist activity" – that concept is limited to "serious" interferences or disruption of "an essential service, facility or system".

Even this more limited phrase was controversial when the Anti-Terrorism Act was drafted after 9/11. An amendment was made while the bill was being debated in November, 2001 to include an exemption for protests or strikes so long as they do not endanger life and regardless of whether they are lawful or not.

In contrast, the only exemption proposed in the new Act is for "lawful" advocacy, protest, dissent and artistic expression."

The government must have known that its approach both to critical infrastructure and the exemption of only lawful protest would be controversial in light of the ATA, 2001 experience and yet they chose to disregard the lessons of the near past.

> g) *interference with the global information infrastructure*

This alone of the 8 subcategories incorporates an existing legislative definition in this case s.273.61 of the National Defence Act as it applies to Canadian Security Establishment Commission (CSE), our signals intelligence agency. This provision does not seem objectionable, and it is unfortunate that its definitional precision and cross-referencing is not found in other parts of the s.2 definition of activities that undermine the security of Canada.

> *h) an activity that causes serious harm to a person or their property because of that person's association with Canada*

This seems to address attempts to harm people or their property because they are Canadian. It would apply to attacks on embassies and perhaps Canadian public or private officials abroad. The Act would allow information sharing both to prevent and respond to such attacks and this seems to be appropriate.

> i) *an activity that takes place in Canada and undermines the security of another state*

This phrase concerns us because it deliberately rejects the more restrictive but still vast (and concerning) definition found in s.2(b) of the CSIS Act, refering to "foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person."

We discuss in our backgrounder #2 on CSIS how this CSIS Act concept – regarded as overbroad by SIRC – becomes particularly troubling when twinned with new CSIS powers proposed by bill C-51. But the CSIS Act at least focuses on Canadian interests and requires that the actions be either clandestine or deceptive or involve threats to person.

In contrast the definition in the proposed information sharing Act means that Canada can share information about even open protests that affect the security of another state, regardless of whether the state is a repressive one. Thus, APEC or Falun Gong type protests might be the subject of information to the extent that they were classified as "unlawful" protests (e.g., done without the proper permit), even if the protests were not clandestine or deceptive and did not involve violence. The effects on diaspora communities may be severe especially if information is shared with immigration officials (one of the 17 listed entities) and potentially with foreign governments.

A limited exclusion of "lawful advocacy, protest, dissent and artistic expression"

This critical exemption or carve out seems to be based on and somewhat broader exemption in the s.2 of the CSIS Act for lawful advocacy, protest or dissent, unless carried on in conjunction with other threats to the security of Canada.

As we discuss also in our backgrounder #2 on the CSIS amendments, the exception is itself limited because of the word "lawful". Something may be unlawful simply because it fails to meet regulatory rules or municipal by-laws – it need not be actually criminal.

Since much protest and dissent can be unlawful, Parliament amended the original 2001 Bill C-36 (Antiterrorism Act), after it was introduced on Oct 15 2001, so that an exemption for protests and strikes removed the qualifier "lawful" in the definition of "terrorist activity". The result is that s.83.01(1)(b) (ii) (E) of the Criminal Code now exempts all "advocacy, protest, dissent or stoppage of work" that is not intended to endanger life.

We believe that as a minimum the exemption in s.2 of the proposed information sharing Act should be as broad as the exemption for protest in the Criminal Code. The Criminal Code exemption recognizes that a free and democratic society should not treat unlawful protests and strikes as national security threats unless they endanger life.

The need for a more robust exemption that excludes unlawful, but non life threatening protests from the information sharing Act is critical because, as discussed above, "activities that undermine the security of Canada" is an infinitely broader concept than the already broad definition of terrorist activity in the Criminal Code or "threats to the security of Canada" in the CSIS Act or "prejudicial to the safety or interests of the State" in the *Security of Information Act*.

C. Section 3 & 4: Purpose and Principles of the Act

Purpose and principles provisions in legislation establish the ill the government seeks to address. Courts asked to interpret ambiguous language in the statute may rely upon purpose provisions.

1. Balanced Legislation Might be Appropriate

We have no problems *per se* with legislation that provides a principled framework for information sharing while recognizing that the sharing of information can also infringe a variety of Charter rights and can harm people (such as Maher Arar) if the information shared is not relevant and reliable. We have not overlooked the fact the fact that the Charter and accountability are mentioned, albeit relegated to a non-enforceable preamble to the Act and not operationalized anywhere.

2. The Act is Not Balanced Between Security and Rights

However, section 3 reveals the unbalanced nature of this legislation when it states that the Act's purpose "is to encourage and facilitate the sharing of information among Government of Canada institutions in order to protect Canada against activities that undermine the security of Canada." In what we have called "Arar amnesia", there is nothing in the proposed act about steps to ensure the reliability and (in any real way) relevance of this information, and no actual facilitation or enhancement of review. Indeed, the concept that only *relevant* and *reliable* information should be shared stressed by the Arar Commission is stretched beyond the breaking point by the needless creation of an overbroad and new concept of "activities that undermine the security of Canada".

3. A Mixed Bag of Principles

Section 4 sets out five principles that should govern information sharing under the proposed Act. The principles are really aspirational as there is no way of actually operationalizing them. Some of the principles seem to contemplate a robust whole-of-government review structure that unfortunately does not exist. As such, the principles are simply a wish list unlikely to be fulfilled. In some cases, the operative parts of the Act actually contradict the platitudes of the wish list.

a) Respect Caveats in Principle while Enabling their Breach

Section 4(b) of the Act notes that respect for originator control and caveats is consistent with the prime purpose of ensuring "effective and responsible sharing" Caveats are restrictions on the further disclosure of information to other parties for other purposes. The Arar Commission found many instances of not placing or respecting caveats in its examination of the information sharing involving multiple Canadian agencies that played a role in Maher Arar's rendition from the US and his subsequent torture in Syria.

There is nothing wrong with the principle of respecting caveats contained in s.4(b) of the proposed Act. Unfortunately it is not enforceable and the principle is overridden

by s.6 of the proposed Act that empowers heads of the 17 institutions or their delegates who have received information under the act to disclose information "to any person, for any purpose." This is anti-caveat language.

The government will argue that we are wrong, and that further disclosures under section 6 must be "in accordance with the law". We will discuss the limited restrictions that this phase may place on subsequent disclosure below in our discussion of ss.5 and 6 of the proposed Act.

At this juncture, we note that caveats and originator control are not law. They are good intelligence practices that recognize the dangers of intelligence collected for one purpose (such as watchlisting) being used for another purpose (such as executive or law enforcement action). So we persist in our argument that section 6 of the proposed act is a statutory approval of potential breaches of caveats. As an authorizing provision, s.6 would trump the unenforceable principle of respecting caveats and originator control contained in the principles of s.4.

b) Information Sharing Agreements and Feedback but No Transparency or Independent Review

Section 4 (c) and (d) refer to the appropriate practices of information sharing agreements and feedback on to the use of shared information. These are good principles, but they are not tied to either review or transparency mechanisms. There is no agreement that information-sharing agreements be public and indeed there are concerns that information sharing agreements including those within the Five Eye partnership are often secret. The feedback that is contemplated would be between the 17 agencies that can share information under the Act. This could improve information sharing, but not in a transparent manner that secures public confidence.

Neither the Auditor General or the Privacy Commissioner named in the government backgrounder as the only reviewers with a whole-of-government mandate have the expertise or mandate to provide the feedback or oversight of information sharing contemplated in the proposed Act's principles. SIRC and other reviewers may have difficulty providing feedback because their jurisdiction is limited to one side of the information sharing relationship.

c) Relevance in a world in which everything is a relevant security matter

The final principle in s.4(e) of the proposed is a very diluted gesture towards the Arar Commission's "relevance" principle. The provision states that only those with jurisdiction or responsibilities relating to "activities that undermine the security of Canada" should have access to information under the Act. The problem is that "activities that undermine the security of Canada" is vastly overbroad. Almost everything, including protests done without municipal permits, could be relevant. Moreover, the expression "jurisdiction and responsibilities" is vast, and whatever constraint might be imposed through judicial interpretation of vague statutory language will be absent. An Act governing internal, secret government information sharing is not something easily brought before a court.

At any rate, none of the "principles" in s.4 are operational legal provisions. At best, they would guide court interpretation of ambiguity in the Act, a form of adjudication that is largely a theoretical possibility with this Act because of the difficulty of people knowing when information is shared about them and bringing effective challenges. As the Arar Commission stressed, self-initiated independent review is essential to achieving principled and balanced information sharing.

D. Section 5: The Authorization of Broad Disclosure

Section 5(1) reads:

> Subject to any provision of any other Act of Parliament, or of any regulation made under such an Act, that prohibits or restricts the disclosure of information, a Government of Canada institution may, on its own initiative or on request, disclose information to the head of a recipient Government of Canada institution whose title is listed in Schedule 3, or their delegate, if the information is relevant to the recipient institution's jurisdiction or responsibilities under an Act of Parliament or another lawful authority in respect of activities that undermine the security of Canada, including in respect of their detection, identification, analysis, prevention, investigation or disruption.

1. An Open Ended List of Government Institutions That Can Share Information

Section 5 authorizes the sharing of information between "government institutions" and 17 are listed in Schedule III. This schedule includes CSIS, CSEC, the RCMP, DND, Public Safety, CBSA, the Armed Forces but also includes Canada Revenue Agency and the Department of Health. This is not an exclusive list as s.10(3) would allow regulations (made unilaterally by Cabinet) adding or deleting from this list.

This list gives us pause. Canada's signal intelligence agency, CSE, is subject to restrictions on collecting information about Canadians, and practices and policies on "minimizing" information on Canadians that it may intercept. How will these existing statutory restriction and policies line up with its inclusion on the list that allows the sharing of information about Canadians in relation to the infinitely broad concept of "activities that undermine the security of Canada"?

The government will note (correctly) that s.5 of the proposed Act subjects the disclosure of information subject to existing legal restrictions. We discuss section 5 and the rigour of its protections further below.

2. Open Ended and Centralized Information Sharing

The open-ended nature of the institutions and the inclusion of 17 institutions in schedule III leads us to conclude that we are very close to a total-information-awareness government.

Given the open ended list of government institutions that can be included and the expansive definition of activities that undermine the security of Canada that includes most public interest matters including financial stability and territorial integrity, the proposed Act creates a unitary approach to government information holding and sharing. [39] Such an approach makes us deeply uneasy. At the very least, Canadians should debate its "big brother" implications.

3. Omission of all but one Review Agencies from Information Sharing

We are struck that the only review agency that is included in the list of agencies that can share information under the proposed act is the Communications Security Establishment Commissioner, listed in Schedule II. This means that the Commissioner may have access to other information even though the Commissioner already has legal authority to access information held by CSE, the only agency that the Commissioner has jurisdiction to review.

This issue raises the important issue that an effective reviewer may need to see both or multiple ends of information sharing relationships. The government's backgrounder stresses that the Privacy Commissioner, the Auditor General, SIRC, and the External Review Committee of the RCMP as well as the CSE Commissioner will all conduct review.

But only the Commissioner is in the information sharing loop under the proposed Act. We don't know why this is, or fully understand the implications. We are left wondering how they will review information sharing if they are not at all ends of the information sharing dyad or triad.

We add that even the inclusion of other review agencies such as SIRC in Schedule II or III and the information sharing loop would be no panacea.

For one thing, it not clear to us that the authority to share information on "activity that undermines the security of Canada" would reach disclosure of information between review bodies on the *conduct and possible wrongdoings* of those agencies who are charged with security functions. That is, the information sharing regime is oriented towards sharing information on the "bad guys" not on sharing information on the bad things that the government might be doing to the "bad guys"

The Arar Commission proposed the creation of statutory gateways that would allow review agencies – including an expanded SIRC and bodies like the CSE Commissioner -- to share information and conduct joint review.[40]

The proposed information sharing bill does exactly nothing on this front. In the result, a law project aimed at an inherently controversial "total information

---

[39] Cohen, above note 13 at 104.

[40] Arar inquiry, Policy report, above note 6, Recommendation 11

awareness" project becomes fundamentally unbalanced and radical legislation. Why do we reach such strong conclusions?

The proposed legislation is unbalanced because it authorizes information sharing without any meaningful enhanced review. The claims in the government's backgrounder that the existing institutions are up to the task is not convincing to anyone familiar with the Arar report.

It is radical because the government has invented a new concept of "activities that undermine the security of Canada" that is much, much broader than any close equivalent, without explaining the necessity or purpose of the new concept.

4. Largely Illusory Restraining Features on Information Sharing

The restraining feature of s.5 is that it does not override other laws. Information also cannot be disclosed under s.5 if it is inconsistent with other provisions or regulations made under this new Act.

This means that prohibitions or restrictions on the ability of an agency to disclose information will remain in effect. This is a good thing, but it begs the question of how much disclosure is restrained under existing laws. Given that the restrictions on information sharing in existing laws are riddled with exceptions and explicit authorization of information sharing, we are not confident that the restrictions on disclosure will effectively restrain the enhanced information sharing under the new Act.

What are the other Acts of Parliament that would restrain the disclosure of information under s.5? Here we must also consider that s.8 of the proposed Act specifically preserves the robust range of both federal and provincial laws authorizing the disclosure of information. This raises the question of the degree to which existing laws both restrain and authorize the disclosure of information.

As noted, the *Privacy Act* only applies to "personal information". While this is a broad concept, we are not persuaded that it reaches all the information whose exchange under the new Act raises concerns. We discuss the "mosaic" concept above.

If it does apply, the *Privacy Act* provides relatively modest safeguards. Section 8(1) has a general prohibition on the disclosure of broadly defined personal information without a person's consent. It then has a long list of exceptions that allow the disclosure of much information.[41]

For example, section 8(2)(a) of the Privacy Act allows subsequent disclosure of information for consistent purpose and use. This is a large exception that government has relied upon for "discretionary latitude to operate effectively within

[41] Craig Forcese *National Security Law* (Toronto: Irwin Law, 2008) at 441-443.

their mandates"[42] but it will become even larger if it is pegged to the definition of activities that undermine the security of Canada.

The Privacy Act also allows disclosure for prosecutorial and law enforcement purposes [43] for research purposes[44] and even for a general reasons where the public interest[45] outweighs any harm to privacy.

Section 8(2) (b) provides another exception "for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure."

Time and space precludes a full survey of the other provisions in Canadian law that authorize disclosure, and therefore are not governed by the *Privacy Act*'s specific disclosure strictures. Suffice it to say that there are many, including under the *Aeronautics Act* (passenger information) and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (financial information).

We have also puzzled over how section 8(2)(b) of the *Privacy Act* will interact with s.10 of the proposed information sharing Act. The latter provision contemplates that the Governor in Council (effectively, the federal Cabinet) will make regulations "for carrying out the purposes and provisions of this Act". As noted, those purposes and provisions are accommodating of information sharing.

Does the proposed legislation write a blank cheque for regulations to expand information sharing in a manner that is then authorized by s. 8(2)(b) *Privacy Act*? We are not sure how to read these statutes together. In the worst case, however, the new Act will constitute the "mack truck" exception to the *Privacy Act*.

Whatever the case, we are sure that regulations can add other institutions to the information sharing list. We are also sure that consequential amendments found in bill C-51 increase what amounts to lawful information sharing under six different existing Acts.

The basic point is that it is mistake to assume that existing or future laws or regulations will place robust restrictions on the disclosure of private information. The larger point is the rules on information sharing are a maze, and this Act contributes to the uncertainty.

5. Enabling Features of Section 5

Although s.5 of the proposed Act seems on its face to incorporate existing legal limits on disclosure and legal limits on the jurisdiction of the 17 institutions that can

---

[42] Cohen, above note 13 at 391

[43] *Privacy Act*, R.S.C., 1985, c. P-21, s.8(2)(f)

[44] *Ibid*, s.8(2) (j)

[45] *Ibid*, s.8(2) (m)

receive information, we are concerned that s.5 may enlarge such jurisdiction in its reference to those institutions being able to use shared information to detect, disrupt, prevent and investigate "activities that undermine the security of Canada".

As discussed above, "activities that undermine the security of Canada" is a new, expansive and we believe overbroad concept. It will be layered over the existing jurisdiction of security agencies such as CSIS, CSEC and the RCMP. At best, this will blur the mandate of these agencies under the information sharing Act with their mandate under existing laws and legal authorities.

At worst, s.5 may be something of a Trojan Horse which will have the effect of *de facto* expanding the range of conduct of the 17 listed institutions to detect, disrupt, prevent and investigate "activities that undermine the security of Canada." We believe that it is not implausible that an official who sends or receives information under the proposed Act will conclude that at the information sharing level at least, and perhaps at other levels, they should be concerned about detecting, analyzing, investigating, preventing and disrupting the broad range of activities that are defined in the proposed Act as undermining the security of Canada.

Even if we are wrong about the above, we still think that that many of the 17 institutions now included in the legislation will experience a disjuncture between their traditional legal jurisdiction and powers and their new information sharing powers that are clearly tied in s.5 to the overbroad concepts of both "activities that undermine the security of Canada" and the undefined and potentially undisciplined concepts in s.5 of "detection" (ie data mining?), "prevention" (by what means?) and "disruption" (without warrant and statutory restrictions?).

Put another way, a lot of information will flow through the system, and it is not clear to us that the instruction that information shared by relevant to each agencies "jurisdiction or responsibilities" will be carefully observed in the hurly burly of real life.

This fear of mandate "creep" might be absolved by a robust review and accountability system. But as noted, we are not convinced that exists. Of the 17 recipient institutions listed in sch 3 only 3 have dedicated review agencies: the RCMP, CSIS and CSEC.

The Auditor General and the Privacy Commissioner have wider remits, but they do not have true jurisdiction or (it seems likely, capacity) to ensure that all these agencies only use shared information in a legal manner.

E. Section 6: The Authorization of Additional Use and Disclosure "In Accordance with the Law…To Any Person, for any purpose"

Our doubts that the limits on information sharing in s.5 are more illusory than real are compounded by s.6. This section provides that once information is received under s.5 it can then be used and further disclosed "to any person, for any purpose" so long as it is "in accordance with law".

As described above, s.6 can be seen as an "anti-caveat" provision that demonstrates wilful blindness about the Arar saga. We are firmly of the view that its deletion should, along with replacement of the overbroad concept of "activities that undermine the security of Canada" be a priority before Bill C-51 becomes law.

In order to understand this awkwardly drafted section, it is best to break it down into its component parts.

1. "in accordance with law"

This is the only restriction on additional use or disclosure of shared information. It is thus an absolutely critical restriction, yet it remains unclear and even opaque.

We think it may refer to the invocation in s.5 to each of recipient institutions acting in accordance with their jurisdiction, responsibilities and lawful authorities. But as suggested above, the *Privacy Act*'s exemptions to privacy are significant. The RCMP has broad authorities not only to enforce the law, but to prevent crime. CSIS has broad responsibilities to investigate threats to the security of Canada, but also ill-defined powers under s.17 of the CSIS Act to disclose information to foreign agencies.

We also believe that "in accordance with law" incorporates the Charter and specifically the restrictions on information sharing in s.7 and s.8. We believe these restrictions could potentially be quite robust. As already noted, information sharing cannot be used to do an "end run" around requirements for warrants, where those would be required by police or intelligence agencies. Nor is information collected pursuant to a warrant then free of constitutional strictures on how it is shared – it must be shared according to a sufficiently precise law, that itself is reasonable, and in a reasonable fashion.

We are, however, quite pessimistic about how the Charter restrictions will be applied and enforced. In the first and in almost all cases, the only Charter review will be done by government lawyers. Their advice will be protected behind solicitor client privilege.

As the Arar Commission found, in many cases a person subject to information sharing will not even know that information about him or her has been shared within the government's ring of secrecy.[46]

2. "using that information"

The 17 recipient institutions are under s.6 empowered to use the information in accordance with law. How would the Ministry of Health or the Canadian Revenue Agency use information shared by for example CSIS or the RCMP about a suspected terrorist? Again the statute is silent and thus opaque.

---

[46] Arar inquiry, Policy report, above note 6 at 490-91.

Will they be tempted to read the references in s.5 to disrupting, preventing, and detecting and do just that - not on the basis of established legal authorities - but on the basis of s.5 of the information sharing Act. Will people named as "people of interest" in an RCMP databank now be audited by tax authorities undertaking their own preventive activities? Will an Aborginal Affairs tidbit on an Aboriginal activist prompt CBSA to indulge is special, secondary examinations at the border? How will all this all-of-government information sharing be coordinated so that an "all-of-government" response to a vastly overbroad concept of security not culminate in a serious of uncoordinated and misdirected agency responses?

Even if courts would read down an adventurous reading of s.6 and insist that all the recipient agencies act according to the existing legal mandates and legal authorities, we are left wondering how such cases will be brought to the attention of the courts. Again, as we have keep restating and as the Arar Commission stressed, those who are subject to information sharing may not even know that that such secret activity occurred. Even if they like Mr. Arar have suspicions and even if they have been harmed by information sharing, it will be uneconomical for them to go to court because s.9 provides that no one can be sued for disclosure of information if they have acted in good faith, which surely must almost always be the case.

3. "disclosing it to any person, for any purpose"

As discussed above, this phrase reflects what we label "Arar amnesia" and empowers recipient institutions potentially to breach caveats that are specifically designed to restrict the subsequent disclosure and subsequent use of shared information. This strikes us as aggressive and provocative legislative drafting. Reasonably informed persons must have known that s.6 would have raised concerns about the possible misuse of shared information. It is with a sense of regret that must as ask ourselves whether this was intended to provoke those most familiar with Mr. Arar's case and those must concerned that it not be repeated in the future. This strikes us as contrary to the spirit of the government's apology and settlement with Mr. Arar.

F. Section 7: Attempts to Shelter Information Sharing from Legal Consequences

Section 7 attempts to limit judicial imposition of new disclosure obligations as a result of information sharing. It is clearly aimed at circumstances where information sharing may be fodder in subsequent criminal trials. For example, it denies a presumption that disclosure of intelligence from CSIS to the RCMP or vice versa means that these agencies conducted a joint investigation. It seeks to stop this Act being used in a way that may trigger disclosure, information sharing and search and seizure obligations under the Charter in criminal trials.

Even with this provision, the ultimate call will rightly be with the courts. They must decide questions of legal privilege and whether the non-disclosure of relevant information threatens a fair trial.

We note, however, that improper conduct stemming from information sharing or the way that information was obtained may be the basis for an abuse of process

motion by the accused.[47] This possibility accords with our concerns, articulated in our backgrounder #2, that much of the Bill C-44 and C-51 package may not have been prepared with adequate attention to knock on effects that new intelligence and information sharing powers may have on criminal trials. Any good defence lawyer must try to mine the information sharing trail leading up to a terrorism arrest in search of Charter violations and other abuses.

The second part of s.7 provides that the sharing of information under the Act will not create a presumption that privilege or of any requirement of consent have been waived. The privileges here could include national security confidentiality privilege or police informer privilege or the new privilege under Bill C-44 for CSIS human sources. With respect to privilege, we reiterate that the courts will make the ultimate decision. Consent waivers likely relate to originator control expectations imposed by foreign intelligence services on information received (and potentially then shared) by the Canadian government. These should be respected even when the legal structures of the act would authorize broader disclosure of foreign-originated information within the Canadian government. Canada is an oft-noted importer of foreign intelligence and s.7(b) recognizes this reality. At the same time, however, it is a reminder that foreign intelligence, while important for Canadian security, may not always be obtained using the same methods as Canadian agencies would use and it may not always be reliable.

The proposed information sharing Act would allow such foreign intelligence to be shared (as it was in the Arar case) but s.7(b) seems to require the consent of the foreign originating agency before the sharing. This, however, could be more clearly stated because we have found the language used in this part of the bill to be confusing.

G. Section 9: No Civil Accountability for Good Faith Information Sharing

As we have repeated several times, the Arar commission found that the courts could not be relied upon to ensure the propriety and Charter consistency of information sharing because a person may not even know that the government was secretly sharing information.

That said, we are troubled by this clause that purports to legislate a very robust qualified immunity should someone (e.g, Mr. Arar or other Canadians tortured in Syria in part because of Canadian information sharing or Mr Abdelrazik who was detained in Sudan) seek to obtain compensation for harms done as a result of "good faith" information sharing. Neither the Arar or Iacobucci commissions found an absence of good faith among government official. It is not clear that s.9 requires only subjective good faith, or conduct that was reasonable in the circumstances at the time.

---

[47] *United States of America v. Khadr*, 2011 ONCA 358 (stay of extradition proceedings because of American misconduct)

Hence, s.9 as presently drafted could preclude most civil recovery should someone in the future be harmed or even killed as a result of the sharing of information, as long as the subjective purpose behind the sharing was earnest, even if the conduct was negligent or ill-executed. Even if courts interpreted good faith to require both subjective and objective good faith, the government is legislating a robust form of immunity.

We also note that s.9 may be unconstitutional if applied to a s.24(1) Charter damage claim[48] arising from information sharing. That said, it could trigger the immunity that applies where a Charter applicant must first establish that legislation is unconstitutional under s.52(1) of the Constitution Act, 1982 before seeking damages under s.24(1) of the Charter.[49]

If enacted, s.9 would bolster the government's argument that a qualified immunity exists because Parliament has authorized information sharing and therefore an aggrieved person must also seek a Constitution Act, s.52(1) remedy against the information sharing Act.

The bottom line is that the act not only does not enhance review and accountability, but it diminishes it with s.9.

H. Section 10: Open-Ended Powers to Enact Regulations

Although we applaud the use of legislation in the national security area and recognize that regulations subsequently enacted by the Governor in Council frequently play a role in legislation, we note that regulations will play an important role in fleshing out the Act with respect to records of how information is shared and adding or deleting recipient institutions. The formal record-keeping requirements may be critical in establishing an audit trail in the (unlikely) event of subsequent review body assessment or judicial review of the information sharing.

The expansion or reduction of recipient institutions also has important policy making dimensions. Schedule III of Bill C-51 should be closely examined because it suggests information sharing for security reasons not only among the usual security players like CSIS, the RCMP, CBSA, CSEC, DND and FINTRAC, but also with health, revenue and finance,

I. Consequential Amendments

We note that six pieces of legislation will be amended to allow new powers of disclosure of information. This demonstrates, again, how vast the practical scope of information sharing is, and how weak the admonishment in section 5 that disclosure be done in compliance with statutes and regulations. For example, the *Income Tax Act* amendments repeal the concept of "designated taxpayer information" which

---

48 *Vancouver v. Ward*, [2010] 2 S.C.R. 28.

49 *Mackin v. New Brunswick*, [2002] 1 S.C.R. 405.

previously restrained the sharing of information to fewer institutions than contemplated in the proposed act.

We are also struck by the different formulations used in the different consequential amendments. The *Excise and Income Tax Act* amendments are tied to "threats to the security of Canada" in s.2 of the CSIS Act and terrorism offences in the Criminal Code, both of which are broad categories but much more restrained that the virtually unlimited concept of "activities that undermine the security of Canada" as defined in s.2 of the proposed information sharing Act. It is the latter, meanwhile, that will be incorporated in the *Fisheries Act*.

How will all this work?

Conclusion: A Concerning Act with Limited Accountability

The proposed *Security of Canada Information Sharing Act* is complex legislation that attempts to cobble together an all-of-government "total information awareness" regime. It is broadly crafted, and arcanely structured. As such it is challenging for the public and even lawyers with extensive backgrounds in national security law to understand. Much more attention has so far been devoted in the debate about Bill C-51 to more easily grasped concept: new criminal offences against promotion and advocacy of terrorism offences, preventive arrests and new powers for CSIS.

But information sharing can have drastic consequences on some individuals and it affects the degree of privacy and freedom that we all enjoy.

If it was law at this time, this new Act would have facilitated the sharing of information about Maher Arar that involved information going from CSIS to the RCMP to Customs and to Department of Foreign Affairs when they had access to Mr. Arar in his cell in Damascus. We are concerned that the enabling nature of the proposed information could authorize a repeat of the Arar saga, as information trickles through the system without serious prospect of being recalled or corrected. The only difference is that s.9 of the proposed act would prevent lawsuits for compensation if officials acted in "good faith".

This proposed Act could affect not only future Maher Arars, but many people who are politically active and engage in dissent. It would do so by authorizing the wide sharing of information related to any "activity that undermines the security of Canada including in respect of their detection, identification, analysis, prevention, investigation or disruption." As discussed above, this can include any of a variety of "unlawful" protests (e.g., without the right permits) related to a broad range of matters including Canada's territorial integrity, its critical infrastructure and attempts to change or unduly influence a government "unlawful means" – a proviso reaching any non-compliance with regulatory rules. Such broad information sharing will threaten and chill rights; it may also drown government departments in so much relatively banal information that they may miss the real threats of serious violence.

And so we are concerned that the proposed information sharing Act will harm privacy and expressive rights and might even harm security. At the same time, conduct under the Act will be difficult to review and scrutinize.

All told, it is difficult to predict exactly all that will happen and all that might go wrong. We are concerned that the government has not tied such a radical Act to a review of its effects and operation after 3 or 5 years operation. Such a review was part of the 2001 Anti-terrorism Act, and was conducted five years after the CSIS Act was introduced (although limited by the inability of Parliamentarian to have access to secret information). It was a process also recommended by the Arar Commission as necessary to complement its much more modest (and rejected) recommendations about improved and enhanced review and accountability in the security sector.

We do not think that a re-consideration years down the road cures all the ills of this Act – many should not be enacted in the first place, and certainly not without a much enhanced accountability superstructure. The government should have responded to the Arar Commission's 2006 report that found review inadequate and it should have responded to the Privacy Commissioner's report released in January 2014 echoing these concerns and calling for legislative enhancements of the *Privacy Act*.

However, if we are moving to a total information sharing era of any sort, as this law appears to suggest, the government should at least mandate some review after 3 or 5 years of the Act's operation. Ideally the review would have an independent investigatory side and a parliamentary side -- and both bodies should have access to secret information. The review should audit how information sharing practices have changed under the Act and their effects on privacy and other Charter rights and on security.