CANADIAN PRIVACY LAW REVIEW

Volume 12 • Number 7 June 2015

In This Issue:

Stumbling toward Total Information Awareness: The Security of *Canada Information Sharing Act*

Craig Forcese
Associate Professor of Law
University of Ottawa

Kent Roach
Professor of Law
University of Toronto

[*Authors' note*: The following is an edited and updated extract of a paper produced in February 2015, responding to the information sharing provisions in Bill C-51. Since producing that paper, we have spent considerable time working out way through the *Security of Canada Information Sharing Act*. The more we probe its details, including amendments that the government had made to it, the more confusing we find its content, and the more difficult it is to predict its consequences. In what follows, we identify our chief concerns.]

Introduction

The proposed *Security of Canada Information Sharing Act* (the "Act") contained as Part I in Bill C-51 is based on the concept of "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 important respects, it comes close to a "total information awareness" approach or, at least, a unitary view of governmental information holding and sharing. In that respect, we consider it a radical departure from conventional understandings of both national security interests and privacy.

LexisNexis®

Canadian Privacy Law Review

The **Canadian Privacy Law Review** is published monthly by LexisNexis Canada Inc., 123 Commerce Valley Drive East, Suite 700, Markham, Ont., L3T 7W8, and is available by subscription only.

Web site: www.lexisnexis.ca

Design and compilation © LexisNexis Canada Inc. 2015. Unless otherwise stated, copyright in individual articles rests with the contributors.

ISBN 0-433-44417-7 ISSN 1708-5446
ISBN 0-433-44418-5 (print & PDF)
ISBN 0-433-44650-1 (PDF)
ISSN 1708-5454 (PDF)

Subscription rates: $280.00 (print or PDF)
$425.00 (print & PDF)

Editor-in-Chief:

Professor Michael A. Geist
Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law
E-mail: mgeist@uottawa.ca

LexisNexis Editor:

Boris Roginsky
LexisNexis Canada Inc.
Tel.: (905) 479-2665 ext. 308
Fax: (905) 479-2826
E-mail: cplr@lexisnexis.ca

Advisory Board:

- **Ann Cavoukian**, former Information and Privacy Commissioner of Ontario, Toronto
- **David Flaherty**, Privacy Consultant, Victoria
- **Elizabeth Judge**, University of Ottawa
- **Christopher Kuner**, Hunton & Williams, Brussels
- **Suzanne Morin**, Ottawa
- **Bill Munson**, Information Technology Association of Canada, Toronto
- **Stephanie Perrin**, Service Canada, Integrity Risk Management and Operations, Gatineau
- **Patricia Wilson**, Osler, Hoskin & Harcourt LLP, Ottawa

Note: This Review solicits manuscripts for consideration by the Editor-in-Chief, who reserves the right to reject any manuscript or to publish it in revised form. The articles included in the *Canadian Privacy Law Review* reflect the views of the individual authors and do not necessarily reflect the views of the advisory board members. This Review is not intended to provide legal or other professional advice and readers should not act on the information contained in this Review without seeking specific independent advice on the particular matters with which they are concerned.

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 vast 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 government's claims that the existing accountability institutions, including the Privacy Commissioner, are up to the task is not convincing to anyone familiar with the Arar report or the Privacy Commissioner's own concerns about the inadequacies of its powers with respect to national security information sharing.

In this article, we first discuss what is at stake in information sharing and argue that the new Act does not give adequate attention to the risks that information sharing presents to privacy or that the sharing of unreliable information can cause injustice. In the second part, we critically examine the new concept of activities that "undermine the security of Canada", which plays a central role in the new information sharing act. In the third part, we examine the most important operative section of the Act. Finally, in the last part, we argue that when the broad information sharing Act becomes law, accountability reform and, in particular, revamped independent review with a whole of government mandate and power will be imperative to counteract the risks of information sharing discussed in the first part of this article.

I. What Is At Stake in Information Sharing

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. But if the objective is antiterrorism, then a law that relaxes rules on information sharing should be about terrorism and should 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 (even factoring in the government's amendment that has expanded the exemption for all advocacy, protest, dissent, and artistic expression, even if it is not "lawful".)

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 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 importantly, integrated information sharing must be matched and balanced with integrated independent review by independent bodies[6] able to self-initiate their own investigations to ensure reliability, relevance, compliance with the *Canadian Charter of Rights and Freedoms* (the "Charter"), and privacy rights. The government has failed to honour these recommendations in Bill C-51.

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, including the exemption for advocacy and protest, 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 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 may well prevent those in Mr. Arar's position from being compensated if they are harmed by the sharing of unreliable information.

Section 6 of the Bill, as originally introduced, authorized disclosure of information (in accordance with the law) "to any person, for any purpose". This section seemed to contemplate 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. The government has amended the section by removing the provocative phrase for further sharing

of information "to any person, for any purpose", but the new section remains awkwardly drafted. When the amended s.6 is read in combination with s. 5, the result is considerable uncertainty about the degree to which the new Act itself authorizes information sharing and the degree to which it requires authorization under existing laws. Government lawyers will have to interpret this act, but given the absence of effective review and inevitable claims of solicitor-client privilege, the public may never know how this act is being applied.

II. The New and Dangerous Concept of Activities That Undermine the Security of Canada

The twin concerns of privacy and injustice discussed in the last section might be tempered by a carefully confined scope of information sharing. Given that the law was enacted in response to the two October 2014 terrorist attacks, one might expect that the act would focus on terrorism. 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 to 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 *Canadian Security Intelligence Service Act* [*CSIS Act*].[7] That definition is broad, and many of its terms are uncertain. It has been criticized for that very reason, including by the Security Intelligence Review Committee. Nevertheless, it 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 the *Security of Information Act*, Canada's official secrets statute.[8]

The New Definition

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 fully.

Instead, the new Act is indexed to an "activity that undermines the security of Canada". The accompanying 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 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" or "chapeau" 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 issues that can fall within the "headline".

We review each the elements of this "headline".

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's 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 (mostly) tying security threats to violence. The definition is imperfect and especially troubling when used as the index for CSIS's new "disruption" powers in Bill C-51. But whatever the shortcomings of the *CSIS Act*, they pale in comparison to the new definition in the information sharing act.

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 with the Supreme Court's recognition that secession from Canada has been a legitimate feature of political debate in Canada.[9]

It must be underscored again that the list that follows the "headline" is merely illustrative. Ultimately, it is the headline that determines the scope of the sharing power. Accordingly, whatever constraint found in the 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 "advocacy, protest, dissent and artistic expression", discussed below.

"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.

The Nine Categories of Activity That Undermine the Security of Canada

The definition then includes an illustrative list of things that, should they meet the "headline" definition, would justify information sharing. 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 the following:

- intelligence
- defence
- border operations
- public safety
- the administration of justice
- diplomatic or consular relations
- 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 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, it's enough for them to involve only "force" *or* "unlawful means" to fall under this provision in the new Act.

We note that "sedition" in s. 59 of the *Criminal Code*[10] 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.[11]

A subversion mandate tied to "force" *or* "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.

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 in the U.K.'s *Terrorism Act, 2000*[12] has drawn much criticism. 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. The government may respond that these concerns about overbreadth are addressed by the exemption for protest, even now unlawful protest. As is discussed in Part 4 of this article, however, this assumes that the protest exemption will be fully and adequately enforced, but that is something that will be impossible to determine in the absence of effective independent whole-of-government review of information sharing practices.

c) Espionage, Sabotage or Covert Foreign-Influenced Activities

This example is relatively unobjectionable, but the concept of sabotage should be more clearly 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".[13] It is, however, a term that has been construed in the case law. The Supreme Court interpreted "terrorism" in *Suresh v. Canada* [*Suresh*],[14] an immigration case. "Terrorism", for the Supreme Court, is intentionally causing death or bodily harm to civilians outside 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 mandates 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 nternational security obligations.

f) Interference with Critical Infrastructure

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*[15] 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 "advocacy, protest, dissent and artistic expression", with no reference to stoppages of work being included.

g) Interference with the Global Information Infrastructure

This alone of the eight subcategories incorporates an existing legislative definition—in this case, s. 273.61 of the *National Defence Act*[16]—as it applies to the Communications Security Establishment Commission (the "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*, referring 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".

The definition in the proposed information sharing Act means that Canada can share information that affect the security of another state, regardless of whether the state is a repressive one, albeit so long as the "headline" definition is met.

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 to the extent they satisfy the vast definition in the Act. 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.

Exemption

The only exemption in the "undermine" definition is for "advocacy, protest, dissent and artistic expression". Initially, this exemption included the qualifier of *lawful* before the list of exempted activities. The word *lawful* provoked controversy during the parliamentary and civil society debates about the bill. "Lawful" conduct would, of course, exclude blockades. It would also exclude workplace strikes inconsistent with labour law, and street protests lacking the proper regulatory permits. Put another way, "lawful" does not mean "non-criminal". It just means without lawful authority.

The risk was that once labour, Aboriginal, or environmental protesters broke one law—including a municipal by-law—they would fall outside the limited safeguards in the new Act.

On this specific question, the government appeared to be deliberately rejecting the compromise approach found in Bill C-36, the original 2001 *Anti-terrorism 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, after controversy, 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.

Predictably, the same controversy reappeared during debate over Bill C-51 ("C-51"). Under pressure from civil society groups (and after having regularly rejected their concerns, sometimes obnoxiously), the government Conservative Party amended the bill in the House of Commons to delete the word "lawful".

We were astonished by this change. We had proposed that "lawful" be dropped but then recommended the same Bill C-36 compromise noted above. That is, we recommended excluding both lawful and unlawful protest and advocacy, but *only* so long as they were not intended to cause death, bodily harm, or endanger life or cause serious risk to health. We think that not all protest and advocacy should be exempted from the new information sharing regime. Violent protest or advocacy of a sufficient scale *can* be a national security issue, justifying information sharing. After all, anyone dimly aware of the history of terrorism appreciates that terrorism can be a form of "protest" or "advocacy", depending on how you define those concepts. Terrorism is certainly a form of "dissent".

But by simply dropping the word "lawful", the new Act seems to preclude new information sharing powers in relation to *any* sort of protest or advocacy or dissent, no matter how violent. And so government officials will now need to spend a lot of time wondering whether, *e.g.*, violent conduct is "protest" or "advocacy" or "dissent", an unnecessary headache that just compounds the incoherence of the Act.

The incoherence of the categorical exemption of all, even potentially violent, protest is troubling. Indeed, it runs the real risk that the exemption in C-51 may simply not be enforced. If true, then the government's defence of C-51 as consistent with democratic freedoms, such as protest, would utterly fail, and we will be left with information sharing based on the broadest possible definition of security that is restricted only by an impractical exemption. An absurd and impractical exemption that includes even violent protest may turn out in practice to be no exemption for even peaceful protest. In any event, it is not certain how or when the public will learn how government lawyers have worked out the dilemmas posed by this amendment and what is now on its face an overbroad exemption for even violent protest.

III. The Working Parts of the New *Information Sharing Act*

Along with the concept of activities that undermine the security of Canada, s. 5 of the Act is the heart of the 10-page act that authorizes information sharing. We quoted s. 2 in full because of its astounding breadth: we quote s. 5(1) in full because of its astounding ambiguity and the many interpretative conundrums it raises. 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.

An Open-Ended List of Government Institutions That Can Share Information

Section 5 authorizes the sharing of information between a "Government of Canada Institutions" listed in the *Privacy Act*[17] (around 100) and the 17 bodies listed in Schedule III of the new statute. 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) to be added to, or deleted from, this list.

Open-Ended and Centralized Information Sharing

Given the open-ended list of government institutions that can be included and the expansive definition of activities that undermine the security of Canada, the proposed Act creates a unitary approach to government information holding. This is a controversial approach. Department of Justice lawyer Stanley Cohen observed in 2005:

> 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.[18]

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—something this new Act risks doing because of the breadth of the "undermine" concept.

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 and how all these authorities will be read with an eye to the new Act. 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.

The *Privacy Act* applies only 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. Consider the implications of whole-of-government information sharing and the "mosaic effect". Government agencies may each individually share pieces of information that 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 may be combined to present a mosaic that does implicate serious privacy concerns. Bits of information that 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, 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.

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.[19]

For example, s. 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 their mandates",[20] 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[21] and research[22] purposes and even for a general reasons where the public interest[23] 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)[24] and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (financial information).[25]

In sum, it is a 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.

Enabling Features of s. 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 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".

We fear 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", "prevention", and "disruption".

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 be 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 we are not convinced that exists, for reasons discussed next.

V. The Unfinished Accountability Agenda

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 underenforced in the absence of integrated and self-initiated review. This is not included in the Bill.

Of the 17 recipient institutions listed in Schedule 3 of the Act, only three have dedicated review agencies: the RCMP, CSIS and CSE.

The government's backgrounder cites the Auditor General and the Privacy Commissioner as "whole-of-government" reviewers.[26] But neither the Auditor General nor the Privacy Commissioner has a mandate to ensure that information sharing is in accordance with all legal restrictions of all sorts.

The Privacy Commissioner himself has raised concerns about the inadequate review structure.[27] Likewise, former interim Privacy Commissioner Chantal Bernier voiced concerns about the "increase[d] surveillance powers without increased oversight structure".[28]

In a 2014 report, the Privacy Commissioner observed:

> [T]he *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 information-sharing has increased greatly.[29]

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 be completed. 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.[30]

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".[31] Leaving aside the merits of the government's defence of new CSIS disruption powers and preventive arrests as subject to judicial control, this judicial involvement is decidedly unavailable to government information sharing.

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, it will be even more 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.

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 had been law at this time, this new Act would have facilitated the sharing of information about Maher Arar, which involved information flowing through 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, at least, parts 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 also 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", subject only to an impossibly uncertain exemption that will be construed, not by courts, but by executive government. The government's deceptively simple amendment that dropped the qualifier that protest must be "lawful" to be exempted makes the exemption available to even violent forms of dissent. This underlines the importance of who interprets this critical provision—it raises the risk that an unworkable exemption may be discounted or even dismissed in practice. The fact that the practice of information sharing will, in many cases, not be subject to independent review means that we may never really know how the new legislation is interpreted and applied by the executive.

And so we are concerned that the proposed information sharing Act will harm privacy and expressive rights and might even harm security. We assert the latter because big data techniques allow the collection and retention of an unprecedented amount of data. This enhanced technology when combined with the overbroad definition of security interests in the *Security of Canada Information Act* may result in massive security files that are stored in electronic warehouses. The needle of actionable intelligence will be more difficult to find in exponentially expanding haystacks. In short, if everything is deemed to be a security matter, then, in effect, nothing may be a security matter—at least, one that will produce actionable intelligence.

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 three or five years. Such a review was part of the 2001 *Anti-terrorism Act* and was conducted five years after the *CSIS Act* had been introduced (although limited by the inability of parliamentarians 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. 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*,

before contemplating legislative on the sharing of security information.

However, if we are moving to a total information sharing era of any sort, as this law appears to do, the government should, at the very least, mandate some review after three or five 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, other Charter rights, and security.

---

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 to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin* (Ottawa: Public Works and Government Services, 2008).

3 Arar inquiry, Factual Report, *supra* note 1 at 365.

4 *Ibid*. at 366.

5 *Ibid*.

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").

7 R.S.C. 1985, c. C-23.

8 R.S.C. 1985, c. O-5, s. 3.

9 *Reference re Secession of Quebec*, [1998] S.C.J. No. 61, [1998] 2 S.C.R. 217.

10 R.S.C. 1985, c. C-46.

11 *R. v. Boucher*, [1950] S.C.J. No. 41, [1951] S.C.R. 265.

12 2000 c. 11, s. 1.

13 *Supra* note 10, s. 83.01.

14 [2002] S.C.J. No. 3, [2002] 1 S.C.R. 3.

15 S.C. 2001, c. 41.

16 R.S.C. 1985, c. N-5.

17 R.S.C. 1985, c. P-21.

18 Stanley A Cohen, *Privacy, Crime and Terror – Legal Rights and Security in a Time of Peril* (Toronto: LexisNexis, 2005): 104.

19 Craig Forcese, *National Security Law* (Toronto: Irwin Law, 2008): 441–443.

20 Cohen, *supra* note 18 at 391.

21 *Privacy Act*, *supra* note 17, s. 8(2)(*f*).

22 *Ibid*., s. 8(2)(*j*).

23 *Ibid*., s. 8(2)(*m*).

24 R.S.C. 1985, c. A-2.

25 S.C. 2000, c. 17.

26 Government of Canada, *Security of Canada Information Sharing Act* (Jan. 30, 2015), <http://news.gc.ca/web/article-en.do?nid=926879>.

27 Office of the Privacy Commissioner of Canada, *Statement from the Privacy Commissioner of Canada Following the Tabling of Bill C-51* (January 30, 2015), <https://www.priv.gc.ca/media/nr-c/2015/s-d_150130_e.asp>. See also *Appearance before the Senate Standing Committee National Security and Defence on Bill C-51, the Anti-Terrorism Act, 2015* (April 23, 2015), <https://www.priv.gc.ca/parl/2015/parl_20150423_e.asp> and *Bill C-51, the Anti-Terrorism Act, 2015: Submission to the Standing Committee on Public Safety and National Security of the House of Commons* (March 5, 2015), <https://www.priv.gc.ca/parl/2015/parl_sub_150305_e.asp>.

28 Chantal Bernier, "Too far, Too Fast?", *iPolitics* (February 12, 2015), <http://www.ipolitics.ca/2015/02/12/chantal-bernier-on-the-terror-bill-too-far-too-fast/>.

29 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), <https://www.priv.gc.ca/information/sr-rs/201314/sr_cic_e.asp> at 5.

30 Arar Inquiry, Policy Report, *supra* note 6 at 291–94.

31 *Ibid*. at 491.