BRIEF TO THE
HOUSE OF COMMONS' STANDING COMMITTEE ON ACCESS TO INFORMATION, PRIVACY AND ETHICS

Analysis and Proposals on the *Security of Canada Information Sharing Act*

November 3 2016

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

Information is the currency of any effective security system, especially one that seeks to pre-empt terrorism. The Air India commission recognized this, and urged that the *CSIS Act* "should be amended to require CSIS to report information that may be used in an investigation or prosecution of an offence either to the relevant policing or prosecutorial authorities or to the National Security Advisor."[1]

The government ignored this recommendation— and despite the occasional puzzling government claims to the contrary, Bill C-51 did not honour it. Instead, Bill C-51 responded to legitimate concerns about siloed information, so evident in the Air India investigation, by throwing wide open the barn doors on information-sharing but in such a complex and unnuanced way that the only certain consequence will be less privacy for Canadians. The Privacy Commissioner has recently warned that "the scale of information sharing that could occur under this Act is unprecedented." It noted that in the first six months of its operation, Canada Border Services Agency, Immigration, Refugees and Citizenship Canada and Global Affairs Canada, three agencies all subject to no dedicated national security review had made 58 disclosures under the new act about individuals suspected of undermining Canadian security.[2]

---

[*] Professor, Faculty of Law, University of Ottawa (cforcese@uottawa.ca).

[**] Professor and Prichard Wilson Chair in Law and Public Policy, University of Toronto, Faculty of Law (kent.roach@utoronto.ca).

[1] Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, *Final Report*, vol. 1 (2010), at 195 (Recommendation 10), online: http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/air_india/2010-07-23/www.majorcomm.ca/en/reports/finalreport/volume1/volume1.pdf. One of us (Roach) was Director of Research (Legal Studies) for this inquiry. In the interest of disclosure, one of us (Roach) was the director of research (legal studies) of this inquiry.

[2] Privacy Commissioner, *Annual Report 2015- 2016*, online: https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/201516/ar_201516

The Privacy Question

Privacy issues figure prominently in discussions of information sharing. The starting point is the federal *Privacy Act*. That instrument says that there is to be "no disclosure" of personal information collected by the government, without consent of the individual concerned.[3] But, as is so often the case, this opening premise is so riddled with exceptions that the exceptions in large measure swallow the rule, or at least complicate it to a considerable degree.

For instance, there is an important exception that basically subordinates the *Privacy Act*: information disclosure is permitted "for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure."[4] Some *Privacy Act*–trumping laws were included in little-noticed amendments contained in the omnibus Bill C-51. (Although, as we discuss below, we think it is untrue that the *Security of Information Sharing Act* is itself a trumping statute.)

All of this would be awkward enough, but on top of these various statutory rules on information sharing, there are also constitutional principles. Law enforcement agencies, for example, may not avoid constitutional search and seizure rules under section 8 of the *Charter* by receiving otherwise protected information from administrative or other bodies not subject to the same constitutional strictures.[5] Where law enforcement agencies propose obtaining private information that is protected by a reasonable expectation of privacy from other bodies, warrants must be obtained, even in circumstances where disclosure of personal information is permissible under the *Privacy Act*.

Likewise, after the Supreme Court's recent decision in *Wakeling*, information collected by warrant retains constitutional protections. If it is then shared without being governed by a clear law, with reasonable safeguards, and in a reasonable fashion, that behaviour too is unconstitutional.[6] *Wakeling* concerned the sharing of intercepted private communications by the RCMP with US authorities in a drug case. The intercepts were authorized under Part VI of the *Criminal Code*, the key wiretap provision in Canadian criminal law. But even so, the case was decided with an eye on Canada's largest post-9/11 scandal: Canada's sharing of false and unreliable information about Maher Arar. As one judge noted, "The torture of Maher Arar in Syria provides a particularly

---

3 *Privacy Act*, RSC 1985, c P-21, s.8.

4 *Ibid*, s 8(2)(b).

5 See, for example, *R v Colarusso*, [1994] 1 SCR 20 at para 93; *R v Cole*, 2012 SCC 53 at para 69.

6 2014 SCC 72 [*Wakeling*].

chilling example of the danger of unconditional information sharing."[7]

CSIS information-sharing, in particular, raises post-*Wakeling* concerns: even as compared with the somewhat sparse language of Part VI of the *Criminal Code*, CSIS information sharing is not governed by a clear law with reasonable safeguards. The *CSIS Act* is permissive without providing the level of safeguards that several of the Supreme Court judges saw as being met by Part VI (which other judges saw as actually insufficient). The exact same comment may be made about the provisions in the *National Defence Act* relating to the Communications Security Establishment (CSE)

And so the *CSIS Act* and *National Defence Act* are out of step with the constitutional standards discussed in *Wakeling*. The result is that these laws will eventually be challenged under the *Charter*, creating further uncertainty about the legality of these agencies' information-sharing activities.

Bill C-51's New Security of Canada Information Sharing Act

The government did not respond to the Air India commission's recommendations or fix the above-noted *Charter* issues with respect to CSIS and CSE information sharing. What it did do was unleash a convoluted new domestic information-sharing law. This law is motivated by a real problem. As correctly noted in an internal CSIS briefing note that pre-dates Bill C-51:

> Currently, departments and agencies rely on a patchwork of legislative authorities to guide information sharing . . . . Generally, enabling legislation of most departments and agencies does not unambiguously permit the effective sharing of information for national security purposes.[8]

The question is, however, what to do about this. As the CSIS briefing note goes on to state, "Existing legislative authorities and information sharing arrangements often allow for the sharing of information for national security purposes. With appropriate direction and framework in place, significant improvements are possible to encourage information sharing for national security purposes, *on the*

---

[7] *Ibid* at para 104.

[8] CSIS, "Memorandum to the Director, Deputy Minister Meeting on National Security Information Sharing" (5 February 2014), CSIS ATIP request 117-2014-393 at 2.

basis [of] existing legislative authorities."[9]

Bill C-51 departs from this advice by superimposing over the existing legal regime a new security information-sharing umbrella law: *Security of Canada Information Sharing Act* (*SoCIS Act*). In so doing, it adds new uncertainty and complexity to the already muddled information-sharing system. That new law articulates a series of generally laudable objectives in its (unenforceable) preamble and "purposes and principles" portions and then presents a series of legal principles that risk creating more problems than they cure.

Astonishing Overbreadth

The Act allows those within the government of Canada to share information about the new and vast concept of "activities that undermine the security of Canada."[10] It is difficult to overstate how broad this new definition is, even as contrasted with existing broad national security definitions such as "threats to the security of Canada" in the *CSIS Act*[11] or the national security concept in the *Security of Information Act*,[12] Canada's official secrets law.

The only exemption in the *SoCIS Act*'s definition of "activities that undermine the security of Canada" is for "advocacy, protest, dissent and artistic expression."[13] This list was originally qualified by the word "lawful", but under pressure from civil society groups, the governing 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 compromise found in the definition of terrorist activity in the *Criminal Code*: we recommended excluding both lawful and unlawful protest and advocacy but *only* so long as it was not intended to cause death or bodily harm, 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 *SoCIS Act*

---

9 *Ibid* at 5 [emphasis added].

10 *SoCIS Act*, above note 7, s 2.

11 *CSIS Act*, above note 4, s 2.

12 RSC 1985, c O-5, s 3.

13 *SoCIS Act*, above note 7, s 2.

seems to preclude new information sharing powers in relation to *any* sort of protest or advocacy or dissent, no matter how violent. Government lawyers will find a way to work around this carelessly drafted exception. Indeed, the government Green Paper has invented a solution: they say that the exception does not include "violent actions".[14] This is not, however, a standard set out in the actual law. It is a policy position – not something that is binding or in the least evident from the actual statute.

Powers to Do What Exactly?

The overbreadth of both the concept of security and the carve-out from it is then compounded by the operative powers in the *SoCIS Act*. In its key operative provision, the Act contemplates that more than 100 government institutions may, unless other laws prohibit them from doing so, disclose information to 17 (and potentially more) federal institutions if "relevant" to the receiving body's "jurisdiction or responsibilities" in relation to "activities that undermine the security of Canada," including "in respect of their detection, identification, analysis, prevention, investigation or disruption."[15] All of these terms are not defined even though they are capable of definition. Without definition, whether by amending the Act or through regulation, there is a danger that many terms in the new Act will be inconsistently applied; a danger that the Privacy Commissioner has already raised.[16]

Relevance or Necessity?

The new act allows information sharing if it is "relevant" to the receiving body's jurisdiction or responsibilities. In plain language, "relevant" here means "having a sufficient bearing on" whatever lies within the agency's jurisdiction or responsibilities. As the Privacy Commissioner noted in his original critique of Bill C-51, much more falls within the orbit of "relevant" than would be captured by the more modest term "necessary." "Necessary" means "needed." The Privacy Commissioner has returned to this theme, critiquing the Green Paper for failing to ask the question whether the low relevance standard should be

---

[14] Public Safety Canada, *Our Security, Our Rights: National Security Green Paper, 2016* ("Green Paper"), online: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016/index-en.aspx ; Public Safety Canada, *Our Security, Our Rights: National Security Green Paper, 2016 Background Document* ("Background Document"), at 29, online: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/index-en.aspx.

[15] *SoCIS Act*, SC 2015, c. 20, s.2, s 5.

[16] Privacy Commissioner of Canada, News Release (Sept 27 2016) online: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2016/nr-c_160927/.

raised to the higher necessity standard.[17] We agree.

Trumping the Privacy Act?

In the absence of a "necessity" requirement, the only safeguard is that the new information sharing power is "[s]ubject 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."[18] We believe that this means that it must comply, among other things, with the *Privacy Act*. That is not an ideal safeguard given the many exceptions in the *Privacy Act*, but it is something.

But we are not sure how to read the government's recent Green Paper documents. They say that because the *SoCIS Act* "authorizes disclosure," it satisfies the "lawful authority" exception to the *Privacy Act*, effectively trumping it.[19] This statement is hard to understand, given that the *SoCIS Act* itself says it is subject to other Acts that "prohibit or restrict" the disclosure of information (and that would include the *Privacy Act*). At the same time, the Paper acknowledges (correctly in our view) that the *SoCIS Act* "cannot be used to bypass other laws prohibiting or limiting disclosure."[20]

Bottom line: the *SoCIS Act*'s entire architecture creates confusion and uncertainty. And in so doing it rejects the lessons from the Arar Commission, Air India inquiry, and the earlier US 9/11 Commission. It threatens privacy as the government seems to want to include almost everything under its radical and novel definition of security interests. At the same time, the *SoCIS Act*'s overbreadth threatens security by making it difficult to focus on terrorism. The Act allows the government to share just about everything while it rejects the Air India commission's recommendation that CSIS *must* share intelligence about terrorist offences, if not to the police than to someone who is in charge and who can take responsibility for the proper use of the information.

If the *SoCIS Act* "works" it will be in spite of its poor and hurried drafting and the short shrift it received as it was rushed through Parliament and its committees in a highly partisan environment. The Green Paper raises another alarm bell. Much will depend on how the *SoCIS Act* is interpreted by the government and the Green Paper suggests that the government is taking an unclear approach in interpreting the Act in its relationship with the *Privacy Act*.[21]

---

17 *Ibid*.

18 *SoCIS Act*, s 5.

19 Background Document, above note 14 at 27.

20 *Ibid* at 30.

21 Craig Forcese and Kent Roach, *False Security: The Radicalization of Canadian Anti-terrorism* (Toronto: Irwin Law, 2015), ch. 5.

What Should Be Done?

It is past time to fix definitively information flows between CSIS and the police. No government is serious about security until it applies itself to this task. This is an issue tied to the intelligence-to-evidence conundrum discussed below, and follows from the Air India Commission's recommendations.

In addition, the government could reduce the complexity (and subjectivity) of its information sharing regime by standardizing national security information-sharing rules throughout the statute books, rather than simply papering over an overly messy system with an even messier umbrella "undermine" concept and a sloppy set of operative rules on disclosure.

Weeding the statute books of conflicting, variable and confusing rules on information-sharing is a worthy task, but it is a task. It will require time and nuance. It is not clear to us that the government will willingly undertake this labour. And so our more minimalist recommendations as these:

- Replace overbroad definition of "activities that undermine the security of Canada" with the more limited and established definition of "threats to the security of Canada" from s.2 of the CSIS Act. This would avoid the radical expansion of security interests currently encompassed by the "undermining the security of Canada" concept.
- As recommended by Privacy Commissioner, amend s.5 to require shared information be "necessary" or "proportionate" and not simply "relevant"[22] to the receiving institution's security jurisdiction
- Amend s.5 to make crystal clear that receiving recipients must operate within their existing mandates and legal authorities and that agencies put in place protocols for ensuring the reliability of shared information, as per the Arar commission recommendations.
- Match information-sharing powers with amendments that give independent review body(s) review over all of the government of Canada's information sharing activities under the new Act. As suggested by the Privacy Commissioner, review should be facilitated by agreements between

---

[22] Privacy Commissioner Submission to the Standing Committee on Public Safety and National Security March 5, 2015 at https://www.priv.gc.ca/parl/2015/parl_sub_150305_e.asp Recommendation 1.

governmental entities that share information.[23] Especially, ensure that this body has the power to compel deletion of unreliable information from all the agencies to which it has been distributed.

- Mirror the exemption to the information-sharing regime on s.83.01(b)(ii) (E) of the *Criminal Code*, thereby exempting "advocacy, protest, dissent, or stoppage of work that is not intended to result in the conduct or harm referred to in any of clauses A to C." (i.e., essentially that is not intended to endanger life, health or safety)
- Implement Recommendation 10 of the Air India inquiry[24] to establish legislated rules in the *CSIS Act* requiring CSIS to "report information that may be used in an investigation or prosecution of an offence either to the relevant policing or prosecutorial authorities or to the National Security Advisor."
- Update *CSIS Act* s.19 and the *National Defence Act* provisions related to CSE so that they comply with the requirements of the Supreme Court of Canada's decision in *Wakeling*.

---

[23] Privacy Commissioner Submission to the Standing Committee on Public Safety and National Security March 5, 2015 at https://www.priv.gc.ca/parl/2015/parl_sub_150305_e.asp Recommendation 4.

[24] Air India Commission, above note 1 at Recommendation 1 and 10, online: http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/air_india/2010-07-23/www.majorcomm.ca/en/reports/finalreport/volume1/vol1-chapt7.pdf