The Criminal Law Quarterly

Volume 60, Number 4 March 2014

Editorial

CSEC's Airport Program: Questions of Legality, Propriety and the Adequacy of Review

The Edward Snowden leaks have revealed that the Communications Security Establishment (CSEC) apparently ran a program that collected metadata on travellers at a Canadian airport. These revelations raise questions about the legality and propriety of CSEC actions in collecting metadata about the addresses and routing but not the substantive content of emails.

CSEC Commissioner Jean-Pierre Plouffe responded within a day of the story breaking with a press release stating that "I am aware of the metadata activities referred to." Although he did not say whether the airport program were legal, he noted that past Commissioners had found metadata collection to be legal. The Minister of Defence has relied on these findings by the retired judges who have been Commissioner to defend CSEC.

The Commissioner issued another statement in February concluding that the CSEC airport program was not directed at and did not track Canadians or constitute "mass surveillance".

The focus of the CSEC Commissioners on legality follow their mandate to report any activities not authorized by law to both the Minister of Defence and the Attorney General of Canada. A failure to report illegal behavior might mean that the Commissioner, who has a budget of $2.2 million compared to CSEC's reported budget of $422 million, missed illegal activities.

The Minister of Defence and the Attorney General of Canada would be obliged to take remedial action if the Commissioner reported illegalities to them, including perhaps even criminal prosecutions if CSEC invaded privacy without legal authorization. This is one of the reasons why the question of legality has gotten so much attention.

Former CSEC Commissioner Decary's June 2013 statements, shortly after the first Snowden leaks, that CSEC had acted legally should be evaluated in light of an extraordinary decision by Justice Mosley in *X, Re*, 2013 FC 1275, 2013 CarswellNat 5304, 2013 CarswellNat 5305 (F.C.). In

declassified reasons released in December 2013, Justice Mosley concluded that CSIS had mislead him by not revealing its plans to draw on the assistance of CSEC's Five Eyes signals intelligence partners in carrying out the surveillance. He called this a "deliberate decision to keep the Court in the dark about the scope and extent of the foreign collection efforts that would flow from the Court's issuance of a warrant." *Ibid.*, at para. 110.

Justice Mosley also concluded that the tasking of foreign agencies by Canadian officials to conduct the surveillance was unlawful. Although the warrants he granted had been used as "protective cover", they did not and could not authorize the use of foreign agencies to conduct surveillance. He concluded that the enabling legislation of CSIS and CSEC should not be interpreted as authorizing requests that would invade human rights and Canadian sovereignty.

Drawing on a SIRC report, Justice Mosley noted that foreign assets had been used in as many as 35 warrants issued since 2009. He indicated that past experience in the Arar and other cases of Canadians tortured in part because of Canadian information sharing underlined the grave risks when Canada loses control over its own intelligence.

Justice Mosley ruled that no reference should be made by CSIS, CSEC or its legal advisors to the erroneous idea that a CSIS warrants authorized the tasking of foreign agencies. This judgment, like some of the American Foreign Intelligence Surveillance Court decisions revealed by the Snowden leaks and subsequently declassified, demonstrates the important role judges can play in supervising surveillance. The BC Civil Liberties Association is currently challenging the constitutionality of the entire CSEC regime under s. 8 of the Charter on the basis CSEC surveillance is authorized by the Minister of Defence and not an independent judge.

Justice Mosley's decision is especially important. He read down the enabling laws of both CSIS and CSEC so as to prevent a transnational accountability gap that would occur if Canada tasked foreign agencies to conduct surveillance of Canadian targets in a manner that effectively left Canada without control of the intelligence produced by its own targeting and tasking. Much of Justice Mosley's bold judgment was premised on the assumption that Canadian tasking of surveillance by its Five Eye partners would violate international law. Unfortunately, the federal government has recently announced that they will appeal this bold decision from a very respected jurist.

Conclusions of legality are only as good as the underlying law. CSEC's mandate is broad. It includes acquiring "information from the global information infrastructure for the purpose of providing foreign intelligence". CSEC's enabling legislation was rushed into law in the months after 9/11. It employs the somewhat old-fashioned concept of prohibiting surveillance that is directed at Canadians or persons in Canada. The internet, however,

largely defies borders especially given the routing of much Canadian traffic. The focus on the government's directions and purpose is at odds with Charter principles that focus on effects on individuals.

The legislation fails to address metadata or the effects of its collection on privacy. The legislation fails to address the incidental interception of Canadian communications that appears to be inevitable given what is known about the big data that can now be collected by signals intelligence agencies. Moreover, CSEC's enabling legislation contained in the *National Defence Act*, R.S.C. c. N, refers only to vague and undefined measures to protect Canadian privacy. CSEC Commissioners have disagreed with government lawyers about how CSEC's ambiguous mandate should be interpreted.

The government is committed to its position that CSEC broke no clear law and did not target Canadians. Others disagree because the targeted airport was after all in Canada. It may be difficult to litigate the issue in open court given the secrecy of relevant authorizations and directives from the Minister of Defence. The underlying issue of privacy, however, is too important to be left to lawyerly sparring.

Canada does not have adequate review mechanisms to ensure the public that its intelligence agencies are adequately doing their job both in protecting security and respecting rights including privacy.

The CSEC Commissioner has a small budget and staff and is restricted by its mandate to focus on questions of legality. Contrary to the Arar commission's 2006 recommendations, the Commissioner cannot share secret information with SIRC even though Justice Mosley's judgment illustrates how the two agencies work together.

Canada's review structure no longer commands the confidence it once did. The last two heads of SIRC have resigned amid controversy, the government abolished the Inspector General who determined the legality of CSIS's conduct and Parliamentary committees are shut out once information has been classified as secret. Wayne Easter's private member's bill would allow Parliamentarians to have some access but would give the Minister's an unreviewable discretion to say no.

Canadians should not stop at the question of whether CSEC's airport program was legal or not. They should demand a more fundamental re-assessment of the law that authorizes CSEC's activities including its treatment of metadata and the increasingly quaint idea that you can collect big data without directing the activities at persons in Canada or targeting Canadians and still not adversely affect the privacy of Canadians. We should also demand that the government revisit the mechanisms that review CSEC activities in light of the Arar Commission recommendations and the recent Snowden revelations.

K.R.