House of Commons Standing Committee on Access to Information, Privacy and Ethics (ETHI)k

British Columbia Civil Liberties Association

Presentation on *Security of Canada Information Sharing Act* (SCISA) (Enacted by Bill C-51)

Dec. 13, 2016

Speaking Notes, Micheal Vonn, Policy Director

Thank you Mr. Chair and members of the committee.

My name is Micheal Vonn and I am the Policy Director of the British Columbia Civil Liberties Association.

I gather that there is a great deal of general agreement among privacy and civil liberties organizations on SCISA. My Association is among the many who have called for the complete repeal of the Act.

Rather than repeat concerns that you are probably familiar with at this stage, I will try to address matters in my prepared remarks that I believe have not had as much discussion, and I hope will assist you in your deliberations.

I will address two matters:

* Firstly, the seriousness of the disruption caused by SCISA’s blurring of the mandates of critically important federal institutions.
* Second, the evidence that rebuts the hope that other legislation will act to moderate the effect of SCISA.

On the first topic, that of the question of mandate, FINTRAC provides a ready example. The Office of the Privacy Commissioner of Canada does intermittent audits of FINTRAC, and these audits have consistently found troubling over-collection and retention of personal data. Obviously there are some discrete remedies available to address some of these issues, as indicated in the recommendations issued by the OPC’s audit report.

But in the main, because the standard of suspicion is very low and the prejudice to individuals extremely high, FINTRAC has long maintained that one of its primary safeguards for privacy is its independence from law enforcement. Now, with the almost unfettered access to information sharing authorized by SCISA, this “independence” is essentially fictional.

The kind of screening mechanism that is the basis for a regime like FINTRAC’s is founded on a necessary balancing. The entire enterprise is one that can only be justified on the basis of a very compelling need. FINTRAC has extraordinary data gathering powers. Personal information that clearly commands a reasonable expectation of privacy is nevertheless compelled by law in such a way that vast over-reporting is a given. Indeed, only the tiniest fraction of reported individuals and entities are found to be conducting themselves unlawfully. To balance that state of extreme prejudice to innocent parties, you must have sufficient counter-balancing protections. The basis of this balancing for the FINTRAC regime is now decidedly unsettled by SCISA, even to the point that its constitutionality may be at issue.

The effect on the mandate of the federal agencies covered by SCISA may indeed be difficult to assess in the short term. But already, the indications are extremely troubling. Because I work in a very broad sphere of rights advocacy, I am in a position to tell you, for example, that health policy advocates are now having to reconsider policy positions and proposals in light of the fact that there is no confidence in the privacy protections afforded to patient information held by Health Canada, because of the sweeping nature of the access that is granted through SCISA.

Even more so, Veterans Affairs is likely to have grave difficulty convincing Canadian veterans that their extremely sensitive and highly prejudicial information, such as physical and mental health information, is appropriately protected. Recall that just a few short years ago, Canada saw its single most appalling medical privacy scandal and it was in relation to veterans’ medical information.

Sean Bruyea, a veteran’s advocate, had his confidential medical files passed around by federal bureaucrats in an apparent effort to discredit him and his advocacy on behalf of veterans. This was a very high profile national scandal in which veteran’s medical information found its way even into ministerial briefing notes.

The unprecedented, all-of-government information sharing capacity afforded by SCISA can only be seen to undermine whatever trust has been re-built between veterans and the federal government since the Bruyea scandal and has an obviously negative impact on the very mandate of Veterans Affairs.

Moving to my second point, I would highlight not only that SCISA has no requirement for individualized grounds and can facilitate the sharing of entire databases, but that it seems likely that it was enacted precisely for the purposes of bulk data acquisition. It does not seem likely that the model of information sharing seen in SCISA is merely meant to address a possible need for clarification of the disclosures permissible under the *Privacy Act*. During the Vancouver Olympics, when the police were discovered to have purchased a military-grade sonic weapon, they said that they were only planning to use it as a large megaphone. And yet, they did not buy a large megaphone, they bought a sonic cannon. Similarly, we did not get an amendment to the *Privacy Act*, we got SCISA.

This fall we have seen a litany of incidents in which CSIS, in particular, has been seen to be unmoored from lawfulness in important spheres of its activity. It must be noted that the alarms and concerns that have been sounded so strongly, not least by the Federal Court, mainly pertain to the collection and use and retention of bulk data.

Sadly, we have learned that s. 12 of the *CSIS Act* (the standard of strict necessity) has proved almost no barrier to CSIS accessing bulk data, as the SIRC audit found (quote): “no evidence to indicate that CSIS had appropriately considered the threshold as required in the *CSIS Act*.”

As a result, it is possible that the vast majority or even EVERYTHING in the CSIS bulk data holdings constitutes illegal spying on Canadians.

It has been argued that the troublingly low thresholds for sharing under SCISA are tempered by the *Privacy Act* and other governing legislation, including the *CSIS Act*. Certainly recent experience gives us no reason to believe that these are operating as meaningful protection. Not only have some of the recently discovered violations of the *CSIS Act* been on-going for over a decade, none have been seen to be remedied. Indeed, there is widespread concern that they will not be remedied and will be condoned by after-the-fact legislation, which will even further corrode public trust in Canadian intelligence agencies.

At this juncture, we have too much evidence to the contrary to accept that SCISA has checks and balances which mitigate the unprecedented scale of information disclosure the Act allowed. The reality is that these purported checks and balances are failing utterly to meaningfully restrain bulk data acquisitions. It is untenable to claim that finding out about a decades’ worth of illegal spying is “the system working”. It is clearly the system not working.

The notion that we have effective limitations on SCISA in other legislation has not proved true thus far, and is not the model that should be applied regardless. It is SCISA itself – which was never justified and actually undermines the very mandates of some of its included agencies-- which must be repealed. Amendments, if clarifications on disclosure powers are needed, should be part of the Privacy Act.

Thank you.