Submission from the British Columbia Civil Liberties Association to The Special Committee to Review the *Freedom of Information and Protection of Privacy Act*

March 15, 2010

Introduction

1. The British Columbia Civil Liberties Association (BCCLA) is the oldest and most active civil liberties organization in Canada. We have spent nearly fifty years working to preserve, defend, maintain and extend civil liberties and human rights in British Columbia and across Canada. We have longstanding and extensive involvement in issues of privacy and access to information, provincially, nationally and internationally.

Focus of this Submission – Privacy

2. The BCCLA is aware that The Special Committee has received numerous submissions making recommendations for improving access to information under the *Freedom of Information and Protection of Privacy Act* (FOIPPA). We concur with all the major themes that have been repeatedly iterated by presenters as to the excessive delays, excessive costs and unwarranted breathe of exceptions in the current FOI regime, and in particular we commend the detailed submission of the BC Freedom of Information and Privacy Association (BC FIPA).

3. We will add only a short item to BC FIPA's concerns pertaining to the obligation to create records, and that is that we have received reports of the use of personal electronic devices as a means of circumventing the Act. We recommend a prohibition on the use of personal electronic devices for government business, except in emergency situations when no other communications device is available.

4. The focus of our submission is the privacy portion of FOIPPA. In particular we wish to call the attention of The Special Committee to the vast citizen data aggregation projects currently underway in British Columbia and the urgent need to update the privacy protections of FOIPPA in light of the unprecedented threats to citizen privacy found in the developing infrastructure for massive data linkages between numerous government ministries.

5. In a democracy, the citizen is sovereign. A very effective way to gauge the health of a democracy is to look at how much privacy is afforded to citizens and how much transparency is required by the government. Our democracy has been under attack in these realms for some time, especially in light of hegemonic notions of "national security" that have been used to argue for ever greater governmental secrecy and wholesale intrusions into citizens' private lives. This would be of serious concern in any era, but with emerging technologies added to the mix, there is now an urgent imperative to re-examine existing privacy legislation in order to create an effective privacy regime for this new environment.

E-health and beyond to the Information Access Layer

6. The government of British Columbia is aggressively pursuing centralization of various types of citizen data. The best known of these projects is the government's "e-health" initiative, which is a centralization of electronic health care records. The provincial e-health project is moving forward despite recent audits by the Auditor General and the Office of the Information and Privacy Commissioner into the electronic health records system of the Vancouver Coastal Health Authority which showed conclusively that the system failed to deliver reasonable security and had absolutely no effective privacy protection. Reforms have been promised, but we have seen many reform promises of late because of the scale and frequency with which privacy scandals are being unearthed, for example, the recent privacy breach affecting 1, 400 income-assistance clients whose personal data was found in the home of a Children's Ministry staff member who has a criminal record for credit card fraud and counterfeiting offences (see: "B.C. response to privacy breach used poor judgment, says review", *Times Colonist*, January 29, 2010).

7. It is inadequate and misleading for the responsible ministries to claim these dire privacy failures are merely the result of isolated cases of poor judgment and various types of inadvertent oversights. Privacy breaches are occurring on an unprecedented scale because electronic records allow for data disclosures on scales never before conceived of. We are not seeing thousands of *paper* files smuggled out of health authorities and ministry office. Electronic records, clearly beneficial in all kinds of ways ranging from legibility to efficient storage, are nevertheless a massive privacy and security liability. And rather than acknowledge and work to minimize these risks, the government is currently building systems and programs that will seriously increase the risks.

8. In the health care field, the envisioned e-health system is meant to centralize citizens' personal health information in a giant data distribution system of interoperable databases accessible from tens of thousands of access points. Under the *E-health (Personal Health Information and Protection of Privacy) Act*, ("e-Health Act") the Minister of Health can create health information banks (HIBs) and HIB administrators have the power to collect patient information from both private and public sector sources. So for example, the first designated HIB, which is the Patient Lab Information System (PLIS), will contain laboratory test results from both private and public sector medical laboratories and e-health, as it is envisioned, is meant to ultimately collect a "Core Data Set" about citizens directly from their private sector family physicians. Once captured in the e-health system, citizens lose all the meaningful privacy protections they have by virtue of the *Personal Information Protection Act* (PIPA) which requires express consent for disclosures outside of the "circle of care". Personal information transferred into the government system becomes subject to FOIPPA which allows for broad sharing of data throughout the government. For more detailed information on the serious patient privacy concerns related to the provincial e-health system, please see attached article entitled "The Real Impact of the E-health Act".

9. The point for our present purpose is to explain the architecture of the e-health system in broad strokes, because the e-health infrastructure is meant to anchor a vast citizen data integration project called the Information Access Layer (IAL).

10. The IAL is a massive information-sharing project, so vast as to encompass the entire public social services sector of the province and linking information about citizens from the Ministries of Employment and Income Assistance, Children and Families, Health, Education, Justice and the private-sector contractors for these ministries. While section 5 of the current e-Health Act does limit the purposes of disclosure of information held in health information banks to purposes that are mostly health care related, we have long suggested that the government may amend that section to allow for a much broader range of disclosure purposes. In our latest communication with government officials on the subject, we were told that the government is currently unprepared to promise that the e-health system won't ultimately be linked to other ministries (communication with Paul Shrimpton, Ministry of Health, Clinical Integration Advisory Council meeting, January 13, 2010). The legislative limitation on disclosure purposes in section 5 of the e-Health Act only pertains to data held in HIBs and only one HIB (PLIS) has been designated. All other citizen health data held by the government and indeed all other kinds of citizens' personal information relies entirely on the privacy protections contained in FOIPPA. And we submit that if those protections were ever adequate, they are no longer so in light of this planned massive, multi-ministry data aggregating project.

11. Privacy-concerned groups have long argued that the "consistent use" provision that allows for data sharing without consent under FOIPPA is too broad. However, before systems developments to effectively link most ministry databases into a giant electronic data distribution system, the extent of data disclosures under "consistent use" would at least be somewhat constrained by the time and effort it would take to isolate, review and send the data at issue. The integration of electronic data systems effectively eliminates this practical check. It is simply impossible to understand the vast monetary investment in this huge data linkage system as predicated on anything other than an assumption of multi-ministry data disclosures as the new 'norm', either under some argument of "consistent use" or under an amendment to the Act.

Recommendations

12. We urge The Special Committee to specifically question the government about its programs for massive citizen data linkages. In our view, the government's proposals to effectively allow for the de facto creation of electronic citizen dossiers through multi-ministry data linkages of often highly sensitive personal information flies in the face of of *Charter* rights and the core privacy principles on which all Canadian privacy legislation is based, including FOIPPA. In addition to our longstanding contention that these types of massive data linkages are simply not possible to implement with reasonable security, the very investment in such a vast infrastructure demonstrates that what the government must view as "consistent use" is so ludicrously vast that the correct scale to

address such use is population-based, not individual-based. The government argues (as always) that its new technology will be more efficient. But the efficiency argument assumes that there are a vast number of multi-ministry disclosures that are required. We believe that such ministry-to-ministry disclosures of personal information must necessarily be rare under "consistent use", because ministries have different mandates which are not obviously "consistent".

13. Therefore, the first privacy recommendation of the BCCLA at this critical time is to put appropriate legislative constraints on disclosures of personal information between ministries. We recommend that FOIPPA be amended so that "consistent use" is clarified to mean only consistent use within the ministry that was authorized to collect the information, and that express consent be required for disclosures of personal information to other ministries.

14. The second privacy recommendation flows from our view that the government be precluded from contractually stipulating that it harvest client data from its private sector contractors who are governed by PIPA. Just as the government of British Columbia is looking to link citizen's personal information held by various ministries, so it is forcefully attempting to collect the client data of private sector service providers who receive any degree of provincial government funding, (see the forthcoming report from FIPA on Integrated Case Management).

15. While the government must naturally have its contractors report on their work, the government only needs de-identified information or statistics. It does not require the personal data of its contractors' clients, many of whom are receiving sensitive services – such as addictions counseling and residence at women's shelters -- that depend entirely on the guarantee of client confidentiality. This attempt to contractually override PIPA is deeply worrying and ripe for legal challenge. While this precise point (government contracts with data harvesting clauses) may be outside the direct purview of The Special Committee, we ask the Committee to recommend an extremely sharp curtailment on disclosures of personal information from private sector providers. If, for example, the government acquires personal information of clients of private sector organization, there must be no further dissemination of that information under FOIPPA without the informed consent of the data subject. This again is especially urgent in light of the development of systems for unprecedented data-sharing within and between various provincial ministries.

16. Finally, in Investigation Report F10-02 Review of the Electronic Health Information System at Vancouver Coastal Health Authority Known as the Primary Access Regional Information System ("PARIS"), (2010 BCIPC 13) at footnote 12, the Information and Privacy Commissioner states that notification pursuant to ss. 23(1)(b) and (c) under PIPA should be required where records contain personal information from both public and private sources. We submit that the Commissioner's views on this matter are correct,

that notification as per PIPA is appropriate in such circumstances and we recommend that such a requirement be codified in FOIPPA.

17. We would be very pleased to answer any specific questions you have regarding this submission or any other aspect of our experience with FOIPPA.

Respectfully submitted,

Micheal Vonn,
Barrister & Solicitor
Policy Director

British Columbia Civil Liberties Association
#550-1188 West Georgia Street, Vancouver, BC, V6E 4A2
604-630-9753