BY EMAIL

Information and Privacy Commissioner of British Columbia
PO Box 9038, Stn Prov Govt
Victoria BC V8W 9A4

July 4, 2011

Dear Commissioner Denham:

Re: ICBC Disclosures to Police of Facial Recognition Data

We are writing on behalf of the British Columbia Civil Liberties Association (BCCLA) and the B.C. Freedom of Information and Privacy Association (BC FIPA) regarding media reports that your office will be auditing ICBC's proposed use of its photo database for the purposes of identifying suspects in the recent Stanley Cup riots. Our associations are deeply concerned about the privacy policy implications of allowing ready police access to the facial recognition-enabled database held by ICBC. In our view, it is arguable that the *Freedom of Information and Protection and Privacy Act* (the "Act") does not provide for the disclosures of personal information at issue and that the deployment of facial recognition technologies raises critical questions that have yet to be assessed in light of the Act.

ICBC's Facial Recognition - Shifting Capacities and Shifting Purpose

In 2009 when ICBC announced that the drivers' license database would be reconfigured for facial recognition capability, the stated purpose for the use of the new technology was fraud prevention. BCCLA and BC FIPA understand that the original 2009 facial recognition system compared photos held within ICBC's database of facial recognition-"readable" photos. This comparison of the facial metrics of license holders was intended to prevent fraud by identifying people with more than one license.

This is not the system, however, that is at issue with identification of subjects in the riot photos, which are obviously photos from 'outside' the database. We were informed by media reporters that ICBC only recently acquired the ability to search the database against a photo that is not already within the system. It is unclear to us how this new

capacity to search the database against external photos could be used for the purposes of preventing licensing fraud, and indeed, we are unaware of any ICBC administrative purpose for such capacity. This raises the concern that ICBC may have developed the capacity for external photo matching with purposes other than its own in mind.

What is the Personal Information in Question?

We have seen various media comments on this issue which emphasize that public bodies are allowed to provide personal information to police for specific investigations and are, of course, required to provide such information on the basis of court orders and warrants. True as these statements are as general propositions, attempting to apply those propositions to the facts of this particular case leads to some serious problems.

Reporters we spoke to on this issue said that ICBC outlined a 2-part process for photo identification. First, the police would give photos for matching to ICBC to run through their system and ICBC would "volunteer" information on which photos they were able to match. Second, the police would seek warrants for those with matches.

This raises the question of the precise nature of the personal information that is being disclosed to police. It does not appear to us that the personal information being disclosed is actually the information that is already held within ICBC's data system and could be disclosed in the ordinary fashion either voluntarily or mandated by a court.

ICBC is not simply disclosing, voluntarily or otherwise, the personal information of John Doe in their database (photo, name, birth date, address, etc.). The entire point of the proposed search of the photo database of British Columbia drivers, is that ICBC is generating an entirely new item of personal information, not held within its own data system – namely that John Doe is (or is not) identified as the person in the photo provided by the police.

This (new) personal information is being generated for purposes entirely outside of the purposes for which ICBC collects personal information and then is being "disclosed" to police. In fact, the 2-part scheme is a distraction from the essential nature of the transaction, which is that ICBC is acting as an arm of the police to search its own database, using surveillance technology that has no clear administrative purpose. ICBC is not "disclosing" information, but rather generating/creating new information (photo matches) which does not exist within its system until a database search is undertaken at police request.

Media Reports

Knowing that our associations' positions are not always accurately reflected in the media, we have been reluctant to accept at face value media characterizations of the OIPC "green-lighting" the police use of the ICBC database. We assume that the OIPC would

be concerned about this proposed arrangement between ICBC and the police, which we do not believe is within the Act. In our submission, the situation is not within the four corners of the law and we believe that the new surveillance technologies that are embedded within the ICBC database change the analysis in important ways.

In our opinion, the proposed ICBC-police arrangements is an attempted end-run around the purposes of the Act and serves as a dire warning about the privacy threats of government/police "cooperation" especially given the greatly intensified data centralization underway in every facet of government service from health care to human resources and ever-expanding surveillance and data-mining technologies that can be used to search those systems.

The media report that the OIPC will be "monitoring" the use of the ICBC database to identify rioters and undertaking an audit of the use of the system. We hope that the concerns we raise in this letter will lead the OIPC to revisit its position on the matter of if and/or how the ICBC-police arrangement fits within the Act. Further, if the OIPC does audit the system, could you please provide us with your audit standards for that review process?

Our associations have had surprisingly strong support for our position on this matter. We are encountering many people who are quickly coming to the realization that the surveillance structures being embedded within governmental service provision are a dire threat to citizens' rights. Many citizens have been shocked to discover themselves de facto criminal suspects, their driver license photos transformed into a mug shot database to be searched at the behest of the police. Many ordinary citizens know well that lines are being crossed and critical rights are in danger.

Yours truly,

Micheal Vonn
Policy Director
BCCLA
Suite 550 – 1188 West Georgia Street
Vancouver, B.C. V6E 4A2
micheal@bccla.org

Vincent Gogolek
Executive Director
BC FIPA
Suite 103 – 1093 West Broadway
Vancouver, B.C. V6H 1E2
fipa@vcn.bc.ca