Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

NEWS RELEASE
For Immediate Release
Feb. 16, 2012

ICBC cannot use facial recognition to identify Stanley Cup rioters without a court order, says B.C.'s Privacy Commissioner

VICTORIA — In a public report released today, Information and Privacy Commissioner Elizabeth Denham found that any use of ICBC's facial recognition technology to identify criminal suspects requires a warrant or court order.

The commissioner launched a systemic investigation into ICBC's use of facial recognition technology shortly after the 2011 Stanley Cup riots, when the corporation offered to match external photographs of alleged rioters against its driver's licence database.

While Vancouver Police did not respond to ICBC's offer in this particular instance, the case raised important questions about the legality of biometric databases compiled by public agencies.

The commissioner established that while ICBC is authorized under the *Freedom of Information and Protection of Privacy Act* (FIPPA) to use the technology for the purpose of detecting and preventing driver's licence fraud, the corporation failed to notify its customers that facial recognition is in use.

"As public bodies implement new technologies that have significant implications for privacy, such as biometrics, the importance of notification is magnified. The public has a right to know this new technology has been implemented and its purpose," said Denham.

Next, the commissioner reviewed ICBC's offer to Vancouver Police, and found that using the database in this manner is not authorized under FIPPA.

"A public body can only use personal information for the original purpose it was collected, except in very limited circumstances. ICBC's offer to use its database to check police-submitted images is clearly a different purpose," said Denham.

The commissioner's findings do not alter the power of police to request personal information from public bodies to assist in a specific investigation, or through the use of a subpoena, warrant or court order, as per section 33 of the act.

"This report sets a very high standard for the use of facial recognition technology, because of the incredibly sensitive nature of biometric data and the very real risk of function creep."

“Facial recognition has the potential to become a technology of surveillance, and we must ensure that public bodies and private organizations using it or contemplating using it have the legal authority to do so along with strong safeguards to protect personal information,” said Denham.

The commissioner made a total of five recommendations, three of which were aimed at improving ICBC’s overall privacy management program.

Summary of Recommendations

1. ICBC should clearly notify customers that facial recognition technology is in use for the purposes of detecting and preventing driver’s licence fraud. At a minimum, notification should be provided at the following points:
    - At all ICBC offices that serve the public .
    - On the ICBC website.
    - In the written notice for renewal of a driver’s licence or identification card.
    - In the application for a new driver’s licence or identification card.

2. ICBC should immediately cease using their facial recognition database to identify persons in images provided by police, unless authorized by a subpoena, warrant or court order.

3. ICBC should establish accountability and leadership on privacy within the corporation, to ensure that privacy is taken into account in decision-making at the executive level.

4. ICBC should implement a privacy impact assessment policy, to set out when and how a privacy impact assessment is completed and reviewed. Technology projects should be reviewed at the conceptual, design AND implementation phases.

5. ICBC should develop a schedule for periodic review of its privacy policies.

The full report can be accessed at: www.oipc.bc.ca

-30-

Media Contact:

Cara McGregor
Manager of Communications and Public Education
Office of the B.C. Information and Privacy Commissioner
250 217-5535