The Facts About Facial Recognition

What is Facial Recognition?
Facial recognition is the process by which a person can be identified or otherwise recognized from a digital image. Facial recognition is one form of biometric identification; others include fingerprints, voice recognition and retinal scans.

Facial recognition is based on unique, measurable characteristics that can be used to verify or recognize identity. When using facial recognition software, the computer takes a picture of an individual and creates a unique numeric representation for the face. This is then compared to a database of facial images, such as a driver's licence database, in an attempt to identify the individual.

Further information on this process is available in Investigation PC-010005-1 from the Ontario Office of the Information and Privacy Commissioner (OIPC) and in Automated Facial Recognition in the Public and Private Sectors, produced by the Office of the Privacy Commissioner of Canada.

How does Facial Recognition Work?
Facial recognition can be used to either confirm (authentication) or discover someone's identity (identification). Authentication is generally used to grant access to facilities or equipment. Identification often involves ensuring public safety, such as maintaining the security of high traffic public places in airports and sports arenas.

The Ontario OIPC discussed this further in Privacy and Biometrics, which was issued in 1999. It explained that the "one-to-many" match is used to identify a person by comparing the image to all others stored in its database. For example, law enforcement may use this strategy to identify criminals. Authentication is a "one-to-one" search where an image on file is compared to the individual; there is no searching or matching to a central database.

Accuracy of Facial Recognition Software
While the use of 3D images has improved the accuracy of facial recognition systems, the risk of false positives (wrong person is identified) or false negatives (a person who should have been identified is not) remains. The accuracy of the match can be impacted by such things as the quality of the image, changes that occur to faces over time and the quality of the algorithm used.

When using facial recognition for identification, the system will search for similar images. This basically places individuals in a "digital line-up". False positives will occur. Identical twins, for example, will probably be flagged each time identification is completed, as there is a second individual in the system with a different name but very similar facial features. In general, facial recognition software is complemented by manual review of matches when such issues arise.

Consistent Use / Scope Creep

By its nature, facial recognition is privacy invasive; it has the ability to identify individuals and link them to other information holdings. Further, an image collected for one purpose could be used for a different purpose without the individual's knowledge or consent. In 2011, rioting broke out in Vancouver after the loss of a game in the Stanley Cup playoffs. The Insurance Corporation of British Columbia (ICBC) offered the use of its facial recognition software to assist police in identifying alleged vandals and rioters.

The Office of the Information and Privacy Commissioner for British Columbia investigated this use in Investigation Report F-12-01, which concluded, in part:

> *I conclude that ICBC must immediately cease responding to requests from police to use the facial recognition database for the purposes of identifying individuals for police absent a subpoena, warrant or court order.*

Use of Facial Recognition in Atlantic Canada for Drivers' Licences and Identification Cards

In Atlantic Canada, facial recognition is being used by provincial governments to confirm the identity of individuals seeking a driver's licence or government-issued photo identification card. Once a photo has been taken, facial recognition software compares the picture of the individual with the picture on file, and searches for other matches to verify the identity of the individual. These actions are intended to reduce the risk of identity theft and fraud and help prevent suspended drivers or fraudsters from getting a driver's licence or photo identification card.

The Information and Privacy Commissioners for Nova Scotia, Prince Edward Island, New Brunswick and Newfoundland and Labrador have each questioned their respective governments on the need for such technology as well as the safeguards needed to protect such information from misuse. They have each committed to monitor and address any further expansion of these programs.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER
NEWFOUNDLAND AND LABRADOR

OIPC Office of the Information & Privacy Commissioner Nova Scotia

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for Prince Edward Island

OMBUD NB N.-B.
LISTEN. REVIEW. RESPOND. ÉCOUTER. ÉTUDIER. CLARIFIER.