Protecting privacy. Promoting transparency.

INVESTIGATION REPORT F12-01

INVESTIGATION INTO THE USE OF FACIAL RECOGNITION TECHNOLOGY BY THE INSURANCE CORPORATION OF BRITISH COLUMBIA

Elizabeth Denham, Information and Privacy Commissioner

February 16, 2012

Quicklaw Cite: [2012] B.C.I.P.C.D. No. 5
CanLII Cite: 2011 BCIPC No. 5
Document URL: http://www.oipc.bc.ca/orders/investigation_reports/InvestigationReportF12-01.pdf

TABLE OF CONTENTS

Executive Summary

[1] Privacy is essential for the well-being of citizens and is a fundamental human right. In British Columbia the rules that protect the privacy rights of citizens are contained in the *Freedom of Information and Protection of Privacy Act* (FIPPA). This investigation report examines the privacy issues associated with the use of facial recognition technology by the Insurance Corporation of British Columbia ("ICBC").

[2] ICBC's facial recognition software came to my office's attention in the aftermath of the Vancouver Canucks' Stanley Cup loss in June, 2011. On the evening of the final game, disappointed Vancouver fans rioted in the streets of downtown Vancouver. Other fans began photographing and posting pictures of the rioters on websites and Facebook pages. The ensuing police investigation included collection of thousands of these images.

[3] In the aftermath of the riots, ICBC offered the use of its facial recognition software to assist police in identifying alleged vandals and rioters.

[4] Our ability to control information about ourselves lies at the heart of the right to privacy. Citizens are entitled to know what information is being collected about them and why. Public bodies must limit the use of personal information to the purposes originally identified unless FIPPA permits a change in use. With the proliferation of new technologies, personal information collected for one purpose may be used to meet new and possibly unanticipated purposes with breathtaking speed and ease. If we are to maintain robust privacy rights, great care must be taken in evaluating proposed changes in use.

[5] Our investigation examined issues relating to both the original intended uses of facial recognition and the proposed use to assist police investigations.

[6] Through this investigation I determined that ICBC adopted and implemented a technical solution that was necessary to address the initial problem it identified—fraudulent acquisition and use of drivers' licences and BCIDs. However, ICBC did not fully satisfy all of the legal requirements when it implemented facial recognition. Specifically, it did not provide adequate notice to citizens. Further, I identified three key areas of ICBC's privacy management program that require improvement.

[7] With respect to ICBC's offer to assist police in their investigation of the Vancouver riot, I determined that the change in use of ICBC's facial recognition database was not authorized under FIPPA. ICBC must receive a warrant, subpoena or court order before it uses its facial recognition software to assist police with their investigations.

[8] 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.

Part 1: Purpose and Scope of this Report

Introduction

[9] On June 15, 2011, the Vancouver Canucks lost in the 7th game of the NHL final and the aftermath of that loss lead us to an investigation into the use of facial recognition technology. Following the 4-0 defeat of the hometown Canucks, Vancouver fans poured out into the downtown streets and some began to vent their disappointment by vandalizing cars and businesses. Others channeled their energies into videotaping and photographing the vandals. Citizen journalism had arrived in British Columbia. Websites and Facebook pages sprouted overnight offering public venues for the display and identification of the images taken by citizens. Police gathered thousands of images of unidentified individuals; many of whom appeared to be engaging in illegal activity.

[10] To assist the police in its investigation of the crimes that were committed that night, ICBC offered the use of its facial recognition software to the Vancouver Police Department.

[11] Following media reports regarding the use of ICBC facial recognition software for this purpose, I took steps to monitor that use. Subsequently, I decided the matter warranted investigation by our Office. Pending the conclusion of this investigation, ICBC agreed that it would no longer accept or respond to any further requests from police.

[12] This report summarizes the results of our investigation into the implementation and use of facial recognition by ICBC and its effect on the privacy rights of citizens.

Investigative Process

[13] Under the *Freedom of Information and Protection of Privacy Act* ("FIPPA") I have the authority to conduct investigations and audits to ensure compliance with any provision of FIPPA.[1]

[1] *Freedom of Information and Protection of Privacy Act*, s. 42(1)(a).

[14] I initially decided to monitor ICBC's use of facial recognition ("FR") technology for the purpose of assisting the police in criminal investigation because of the privacy issues raised by that change in use. As part of that monitoring process, we met with ICBC officials on July 15, 2011, and were provided with a demonstration of the technology, further details of the history of the implementation of ICBC's facial recognition technology and proposed processes for sharing information with the police. Because of information received at that meeting, and as a result of receiving a number of complaints regarding the proposed use of ICBC's FR technology by police, I decided to conduct a broader investigation into ICBC's use of this technology.

[15] During our investigation, we asked ICBC to respond to a series of questions. We also requested documentation in support of its responses and conducted three site visits to independently verify select components of ICBC's privacy and security program. In addition we conducted research on facial recognition with a view to acquiring a better understanding of the privacy and security issues associated with the implementation and use of FR technology.

Application of FIPPA

[16] ICBC is a Crown corporation listed in Schedule 2 of FIPPA and as such is a "public body" within the meaning of FIPPA. One of the purposes of FIPPA is to protect personal privacy by preventing the unauthorized collection, use or disclosure of personal information by public bodies.[2] We examined ICBC's implementation of facial recognition technology and its offer to share that information with the Vancouver Police Department in light of the rules set out in FIPPA.

Background

[17] Facial recognition technology was implemented following a significant evaluation beginning in November 2008 with a project known as the "customer Identity Verification Feasibility Project" ("Identity Project"). The purpose of the project was to enhance the security of British Columbia drivers' licences ("BCDLs") and British Columbia Identifications ("BCIDs")[3] by detecting and preventing fraudulent use or obtaining of these documents.[4]

[18] The Identity Project evaluated the three types of identification fraud: fake identification, stolen identification and false identification.

---

[2] FIPPA, s. 2

[3] BCIDs are identification cards intended for non-drivers who require a legal piece of identification. BCIDs are typically used in any situation where a driver's license would be used for identification. Anyone 12 years or older can apply for a BCID.

[4] ICBC Response to OIPC Investigation, August 31, 2011, p. 5.

[19] Fake identification is identification using replica and home-made versions of official documents. Stolen identification is self-explanatory. False identification refers to legitimate identification falsely obtained. That is, individuals obtain identification directly from federal and provincial organizations under a false name.

[20] The Identity Project determined that the annual costs of identity fraud in 1998 could conservatively be estimated at $90 million.[5] This did not include the costs associated with accidents caused by unqualified and disqualified drivers. One of the key challenges in dealing with false identification was the fact that, in 1998, there were 3.5 million active driver's licences and approximately 600,000 BCIDs. While ICBC officials could easily visually compare Bob K. Smith's present photograph with the image stored for Bob K. Smith from his last driver's licence renewal, ICBC did not have any process to accurately determine whether the image of Bob K. Smith matched with any of the other 4 million images in its database.

[21] The Identity Project formulated a variety of strategies to address the problem of identity fraud. Most of these strategies were implemented. However, ICBC determined that only an automated system capable of comparing millions of records could address the issue of multiple identity fraud.

[22] As a result, in November 2008, ICBC implemented FR technology. Using this technology, a facial recognition template (FR template) is created for each image. Each FR template is unique to an individual image and can be compared by the computer software, against all other templates to determine whether or not an individual template is a potential match to other templates in the system.

[23] Currently, there are approximately 3.1 million active BC driver licences and 455,000 active BCIDs[6]. All of these drivers and BCID holders have an FR template stored in ICBC's database. When any individual applies for a new or replacement DL or BCID, his or her picture is taken and a new FR template is created. That template is compared against all of the existing templates to determine whether the individual is who s/he says s/he is and also to determine if perhaps the individual has more than one identity. There are currently 4.4 million FR templates in the repository.[7]

---

[5] CIV Project Report – A review of the Extent of Identification – Related Fraud in British Columbia, December 7, 1998, p. 101.

[6] The most current numbers available from ICBC were 3.1 million active driver licences and 455,000 active BCIDs. These numbers are from 2010.

[7] There are more templates in the FR repository than there are active driver licenses and BCIDs because the repository includes templates for expired, cancelled and suspended driver licenses and BCIDs.

[24] In the fall of 2010, ICBC purchased an enhancement to its FR technology. The enhancement included both the ability to import images and the ability to adjust the error margins/threshold used to compare those images to other images in the database. The ability to import images meant that ICBC could apply the technology to images from sources other than ICBC's own digital picture identification database.

[25] ICBC advised that the enhancement was purchased at the request of the Integrated Municipal Provincial Auto Crime Team ("IMPACT"). IMPACT is a joint law enforcement initiative funded by ICBC. It is known mainly for its bait car program which involves setting up cars with hidden cameras used to catch thieves as they attempt to steal the bait car. Officials with IMPACT had hoped that ICBC could use its FR technology on photos taken by bait car cameras to identify car thieves. Following the purchase and installation of the enhancement, ICBC received a total of 15 requests from law enforcement agencies to use FR technology.

[26] No requests were received as a result of the offer made to the Vancouver Police Department following the Stanley Cup riots of June 15, 2011. Pending the conclusion of this investigation, ICBC decided that it would no longer accept or respond to any further requests from police.

Issues

[27] The issues in this investigation are:

1. Is biometric data personal information?

2. Is collection of data for facial recognition authorized?

3. Does ICBC's notification to client/citizens satisfy the requirements of FIPPA?

4. Does use of personal information in the operation of ICBC's facial recognition software comply with FIPPA?

5. Do the steps taken by ICBC to protect personal information held within ICBCs' drivers' license database, and that are used in the operation of FR software, comply with s. 30 of FIPPA?

6. Does disclosure of personal information to police, following confirmation that ICBC's FR software has matched a photograph with a record in the drivers' licence database comply with FIPPA?

Part 2: Facial Recognition and the Right to Privacy

Privacy Rights of Citizens

[28] One of the purposes of FIPPA is to protect personal privacy. In order to understand the significance of FR technology it is important to first outline what this right to privacy means.

[29] Privacy is a complex idea. The boundaries of what is private and what is public can shift according to individual opinions and circumstances.[8]

[30] The significance of the privacy rights of citizens in a free and democratic society was eloquently stated by Mr. Justice La Forest,

> [Privacy] is at the heart of liberty in a modern state. Grounded in man's physical and moral autonomy, privacy is essential for the well-being of the individual. For this reason alone, it is worthy of constitutional protection, but it also has profound significance for public order. The restraints imposed on government to pry into the lives of the citizen go to the essence of a democratic state.[9]

[31] In the recent decision of the Ontario Court of Appeal in *Tsige v. Jones* the court examined the meaning of privacy. In deciding that the tort of invasion of privacy or "intrusion of seclusion" exists, the court highlights the significance of technological developments:

> [67] For over one hundred years, technological change has motivated the legal protection of the individual's right to privacy. In modern times, the pace of technological change has accelerated exponentially. Legal scholars such as Peter Burns have written of "the pressing need to preserve privacy" which is being threatened by science and technology to the point of surrender"... .[10]

[32] Under FIPPA, privacy means maximizing a citizen's control over the collection, use and disclosure of his or her personal information whenever

---

[8] In her work "Privacy in Context: Technology, Policy and the Integrity of Social Life", Helen Nissenbaum discusses the complex series of factors individuals take into consideration when deciding what information to keep private and what information to disclose. The factors include roles, activities, norms and values. In the course of reviewing hundreds of individual privacy complaints each year, we see that individuals make decisions about what should and should not be private taking into account these complex factors.

[9] *R. v. Dyment* (1988), 45 C.C.C. 93d, 244 (S.C.C.), at para. 17.

[10] *Tsige v. Jones* 2012 ONCA 32, at para. 67.

possible and to the extent that is reasonable.[11] Public bodies are accountable to the public and must collect, use and disclose personal information in accordance with the rules and standards set out in FIPPA.

[33] The Organisation for Economic Co-operation and Development ("OECD") is an international forum that sets international standards to promote the economic and social well-being of people around the world. The OECD has described privacy as the right to do the following within the bounds of the law:

- To keep our personal information to ourselves;
- To remain anonymous or unidentified with respect to certain personal and public activities if we choose;
- To live our lives without being under surveillance;
- To conduct private communications;
- To have physical privacy and personal space, and
- To be left alone both as consumers and as citizens.[12]

[34] What is important to recognize is that privacy is a right enshrined in FIPPA. It has depth and complexities, it is articulated in standards and rules that govern the activities of public bodies. Citizens have the right to rely on the protections afforded under FIPPA, especially as new technologies stretch our understanding of these rules.

Facial Recognition

[35] "Biometrics" is literally, the measurement of life. It refers to the technology of measuring, analyzing and processing the digital representations of unique biological data and behavioral traits such as fingerprints, eye retinas, irises, voice and facial patterns, gaits, body odours and hand geometry.[13]

[36] This measurement can be used in two ways. First, it can answer the question, "Is this person who s/he claims to be" by comparing the new measured biometric against one known to come from a particular person (a one-to-one comparison).[14] Secondly, it can answer the question, "Who is this person" by

[11] Former Commissioner Loukidelis made a similar comment with respect to the meaning of privacy under PIPA in his general briefing to the Special Committee to Review PIPA on May 29, 2007.
[12] Directorate for Science, Technology and Industry Committee for Information, Computer and Communications Policy, Working Party on Information Security and Privacy, Organisation for Economic Co-operation and Development, "Biometric-Based Technologies", 30 June 2004, DSTI/ICCP/REG(2003)2/FINAL, at p. 6.
[13] Btihaj Ajana, "Recombinant Identities: Biometrics and Narrative Bioethics", Bioethical Inquiry (2010) 7:237-258 at p. 238.
[14] Mordini and Petrini, "Ethical and social implications of biometric identification technology" Ann 1st Super Sanita 2007, Vol. 43, No. 1: 5-11 at p. 5.

comparing a new measured biometric against a database of stored records (a one-to-many comparison).

[37] Facial recognition identification occurs in the following stages:[15]

1. **Enrolment**: A digital photograph is taken of the face. Measurements are taken from the photograph. ICBC uses software that combines face geometry measurements and skin texture analysis. The measurements are put into mathematical formulas (algorithms) that convert the measurements into a binary code—a number consisting of a series of zeros and ones unique to each individual image. This binary code is known as the facial recognition template (FR template).

   When the technology was implemented by ICBC, the most current image of all BCDL and BCID holders already present in ICBC's database were entered into the facial recognition software system. In other words, all BCDL and BCID holders were "enrolled" and an FR template was created for each.

   Each time an individual in BC applies for a new or replacement BCID or BCDL, a new image is taken and a new FR template is created from that image.

2. **Storage**: The produced FR template can be stored in a database or on other forms of digital media such as a chip card. In ICBC's case the FR template is stored in a database.

3. **Matching**: If the individual is renewing or replacing existing identification, ICBC conducts a one-to-one comparison of the newly created FR template against the FR template associated with their existing record. If the person is who s/he says s/he is, then the FR templates should match and the original images should be of the same individual. ICBC also conducts a one-to-many comparison for all images to determine if the individual has more than one identity in the system.

   The one-to-many comparison is significant from a privacy perspective. This comparison requires that the unique binary code of the individual in question is compared against every one of the 4.4 million FR templates in the repository. The FR software evaluates the potential matches and assigns a score. The higher the match score, the more similar the photos are.

[15] Btihaj Ajana, "Recombinant Identities: Biometrics and Narrative Bioethics", Bioethical Inquiry (2010) 7:237-258 at p. 238.

In ICBC's case, where the system identifies a potential duplicate a subsequent level of investigation is required by the Licensing Fraud Group. Each morning, lists of potential matches are sent to this group. Two FR investigators independently review the potential matches by viewing the associated photographs. They both must independently judge whether the photographs are a match or not. In this double blind analysis, they are unaware of each other's assessment.

While the technology itself can be fairly simply explained, once implemented it can accurately be described as obscure and opaque. Facial recognition requires no participation or consent from individuals. The software is applied to photographs that individuals may or may not know have been taken. The software algorithms are complex mathematical formulas that most people cannot understand. Even if an individual were to go through the software code line by line it would be impossible to trace the connection between the code a person inspected and the code being executed by the software program.[16]

Potential Concerns with Facial Recognition

[38] Facial recognition has the potential to assist in protecting individuals against identity theft. Properly implemented, the software can be used to quickly and efficiently compare millions of images to determine whether an individual is who she says she is. Identity theft is becoming increasingly common in our society and it can have serious negative consequences including bank fraud, loan fraud, credit card fraud and document fraud. Recent statistical information shows that Canada's largest credit bureaus, Equifax and Trans Union, receive over 1,800 identity theft complaints from Canadian citizens every month.[17]

[39] However, FR technology has also been described as "one of the gravest privacy threats of our time."[18] Privacy experts, particularly in Europe and North America, have identified a number of significant privacy concerns associated with FR technology.[19] The two most significant ethical and privacy implications of biometrics are function creep and the use of our bodies as identification tools.

---

[16] Lucas D. Iatrona, "Disclosive ethics and information technology: disclosing facial recognition systems", Ethics and Information Technology (2005) 7:75-86 at p. 77.
[17] "Identity Theft FAQs for Canadians", http://www.identitytheftfaq.ca/
[18] Amber Yoo, "Facial Recognition: A Top Privacy Issue of Our Time", http://www.californiaprogressreport.come/site/print/9298.
[19] Appendix C to this report provides a brief summary of a number of privacy concerns including such things as clandestine tracking, over collection, interoperability and accuracy. Appendix C also contains a brief bibliography of articles discussing the ethical and privacy concerns associated with facial recognition technology.

[40] Facial recognition is now available on social networking sites, has been implemented on video surveillance cameras and used at large public events to identify attendees.[20] With the implementation of facial recognition individuals will no longer be able to remain anonymous in public places. The system may, in a matter of seconds to minutes, identify you to the public body or organization running the facial recognition software. Previously private political, religious and social affiliations will now become public.

[41] **Use of our bodies as identification tools**—FR technology has the potential to change our relationship with the world. Deciding what information about ourselves we will share with others helps define the boundaries of different relationships. One shares more of himself with a friend than with an employer, more with a life-long friend than with a casual acquaintance. The ability to keep parts of our lives private is central to our ability to feel unique—when our lives are laid bare for all the world to see, we can take no more ownership over them than anyone else.[21]

[42] It is also important to recognize that collecting biometric features means collecting data of the *body of a person.*[22] The significance of biometrics is aptly stated by Professor Alterman, Department of Philosophy, Baruch College, C.U.N.Y states:

> Biometric data acquires a fundamental privacy interest because it has an impact on one's right to control the use and disposition of one's body. With biometric identification, the image is a tool, the purpose of which is to permit recognition of the body by external entities that have an interest in it. Offering up this "piece of yourself" authorizes and enables others to use your body for purposes of their own. It thereby objectifies the body by isolating the physical element from the person and providing it as a means to an end in which the person has no inherent interest. The body becomes an object whose identity is instantly determinable by purely mechanical means, and subject to external controls on that basis; while those means themselves are removed from the control of the subject. The representations are infinitely reproducible by their owner, but are not even accessible to the subject whose body they represent. The embodied person now bears, more or less, a label with a bar code, and is in this

[20] Facebook introduced photo recognition into its photo application in June of 2011. USA Today reported in May 2007 that Homeland Security was investing heavily in research into facial recognition technology for video surveillance cameras. One of the earliest publicly known implementations of facial recognition technology in video surveillance was at the 2001 Superbowl in Tampa Florida.

[21] "In the Face of Danger: Facial Recognition and the Limits of Privacy Law", 120 Harvard Law Review 1870 (2007) at 1887.

[22] Article 29 Data Protection Working Party, "Opinion 3, 2005 on Implementing the Council Regulation (EC) No. 2252/2004 on standards for security features and biometrics in passports and travel documents issued by Member States, Official Journal L385, 29/12/2004 p. 1-5" 1710.

> respect alienated from her own body as well as from the technology used to recognize it.[23]

[43] Understanding that biometrics are intimately related to our identity and our ability to control information about ourselves is important in appreciating how sensitive the information is. Under FIPPA, the head of the public body has to exercise discretion in a number of instances, including in determining what is "reasonable" in terms of the security arrangements that are in place to protect personal information and whether to disclose information in response to requests from other public bodies. The sensitivity of the personal information is relevant to both when and how to exercise discretion and to what is "reasonable" in the circumstances.

[44] **Function creep**—Function creep occurs when a process or system intended for one purpose is subsequently used for a new or originally unintended purpose. When personal information is involved, function creep implies that the change in use is without the knowledge or consent of the individuals.

[45] Function creep is a particular concern in biometrics because biometrics is a very powerful identification tool and because databases are becoming increasingly interoperable.

[46] Currently, a very common use of biometrics, particularly facial recognition, is migration management. In Europe, facial recognition is commonly used at borders to determine the identity of individuals attempting to immigrate to Europe. A major concern is that data collected for immigration management purposes will subsequently be used for the prevention and detection of crime.[24] New ISO standards of interoperability at the international level mean that the biometric industry is increasingly moving towards worldwide applications for biometrics.[25] This adds to the concern because biometric templates collected in one system could well be comparable to templates collected in another.

[47] Function creep is a privacy issue because it is a basic privacy principle that personal information should only be used for the purpose it was originally collected unless, in the case of public bodies, FIPPA permits a change in use. Such a change in use should be subject to careful scrutiny given the sensitivity of biometric data and its potential for interoperability with other systems.

---

[23] Anton Alterman, "A piece of yourself": Ethical issues in biometric identification", Ethics and Information Technology (2003) 5: pp. 139-150 at pp. 145-146.

[24] Jillyanne Redpath, "Biometrics and international migration" (2007) Ann 1st Super Sanita 2007, Vol. 43:No. 1, 27-35 at p. 31.

[25] ISO/IEC 19794-5, Information Technology – Biometric Data Interchange Format – Part 5: Face Image Data.

[48] ICBC's initial implementation of FR software was strictly intended for the internal use of the corporation. However, understanding the full potential implications of this technology is helpful in evaluating its significance and in predicting possible future uses. Our investigation examined issues relating to both the original intended purposes of facial recognition software and the proposed use of the software to assist police investigations.

Part 3: Facial Recognition and Compliance with FIPPA

[49] In the course of our investigation we examined six issues relating to ICBC's implementation and use of FR technology and its compliance with the rules under FIPPA:

1. Is biometric data personal information?
2. Is collection of data for facial recognition authorized?
3. Does ICBC's notification to client/citizens satisfy the requirements of FIPPA?
4. Does use of personal information in the operation of ICBC's facial recognition software comply with FIPPA?
5. Do the steps taken by ICBC to protect personal information held within ICBCs' drivers' licence database, and that are used in the operation of FR software, comply with s. 30 of FIPPA?
6. Does disclosure of personal information to police, following confirmation that ICBC's FR software has matched a photograph with a record in the drivers' licence database comply with FIPPA?

Meaning of "Personal Information"

[50] In my view, biometric data used in ICBC's facial recognition software application is personal information under FIPPA. "Personal information" is defined in FIPPA as recorded information about an identifiable individual, other than contact information.[26] There is no doubt that a digital photograph of an individual is that individual's personal information, but the issue is whether measurements taken of an individual's face geometry, facial features and skin texture and patterns are personal information. The measurements form the basis of facial recognition because, taken together, they can be used to identify one individual among millions.

[26] FIPPA, Schedule 1

[51] The European Union, Data Protection Working Party states in its foundational discussion paper on biometrics:

> "…measures of biometric identification or their digital translation in a template form in most cases are personal data. It appears that biometric data can always be considered as 'information relating to a natural person' as it concerns data, which provides, by its very nature, information about a given person. In the context of biometrical identification, the person is generally identifiable, since the biometric data are used for identification or authentication/verification at least in the sense that the data subject is distinguished from any other."[27]

[52] There is no doubt that biometric data relates to an identifiable individual. I conclude that the measurements taken, and the unique biometric template created by applying the algorithm to the measurements, is personal information within the meaning of FIPPA.

Collection of Personal Information

[53] Does collection of personal information for the purposes of determining whether a photograph matches a record in ICBC's driver's licences database comply with ss. 26 and 27 of FIPPA? FIPPA provides that a public body may only collect personal information in eight enumerated circumstances.[28]

[54] ICBC relies on s. 25 of the *Motor Vehicle Act* and ss. 3 and 4 of the Voluntary Identification Card Regulation as express authority to collect personal information, including digital images in order to issue BCDLs and BCIDs.[29] Under FIPPA, a public body may collect personal information where the collection of information is "expressly authorized under an Act".[30] I agree that ICBC has the express statutory authority to collect digital images for the purposes of issuing BCIDs and for the purpose of determining an applicant's driving experience, driving skills, qualifications, fitness and ability to drive and operate any category of motor vehicle designated for that class of driver's licence for which an application is made.[31]

---

[27] Article 29 Data Protection Working Party, "Working document on biometrics" (1993), 12168/02/EN WP80 at p. 5.
[28] Prior to amendments to FIPPA that came into effect on November 14, 2011, there were only three permitted purposes for collection of personal information, one of which was statutory authority.
[29] See Appendix 1 for copies of the relevant statutory provisions.
[30] FIPPA, s. 26(a).
[31] These purposes are set out in s. 25(3) of the *Motor Vehicle Act*.

[55] Although the collection of digital images of citizens is authorized, does the manipulation of these images result in the collection of new information?

[56] The FR software implemented by ICBC, takes a series of measurements of the subject's face from the digital image captured by ICBC. Another way to describe this is that ICBC manipulates its electronically stored image data to produce a new electronic image—a binary code representation of the digital image known as the FR template. In the course of applying the FR software to the digital images, ICBC does not acquire any new personal information that it did not already have in its possession. So, while the FR software allows ICBC to take measurements of an individual's face, the size and shape of the face were already contained in ICBC's database. The new software simply allows ICBC to conduct the measurements.

[57] I find that the manipulation of existing data using facial recognition software does not result in the collection of new personal information but does involve a **new use** of personal information that must satisfy the requirements of s. 32 of FIPPA.

Notification Requirements

[58] In interpreting FIPPA, its language is to be read in its grammatical and ordinary sense and its entire context, in harmony with FIPPA's scheme, its objective and the intention of the Legislature.[32]

[59] Section 2(1) articulates the purposes of FIPPA. They are to make public bodies "more accountable to the public" and to "protect personal privacy". FIPPA's privacy protection goal is achieved, among other things, "by preventing the unauthorized collection, use or disclosure of personal information by public bodies".[33]

[60] While it is generally understood that public bodies are made more accountable to the public mainly through the access provisions of the Act, the notification provision in s. 27 is also an important accountability mechanism. Without notification, individuals would be unaware of the types of personal information collected and the purposes for the collection and so would be unable to take advantage of their rights to access the information and to request correction or annotation of the information.

---

[32] See, for example, *Rizzo & Rizzo Shoes (Re)*, [1998] 1 S.C.R. 27, applied in, for example, Order 02-38, [2002] B.C.I.P.C.D. No. 38. Also see s. 8 of the *Interpretation Act*.
[33] Section 2(d) of FIPPA.

[61] As public bodies implement new technologies that have significant privacy challenges and implications (such as biometrics, or Smart Meters[34] or data linking, data sharing projects), the importance of notification as an accountability mechanism is magnified. The public has a right to know that this new technology has been implemented, the purposes for the implementation and contact information for citizens to call with their questions. Proper notification is an opportunity for public bodies to ensure that they address some of the fundamental privacy interests associated with biometric data.

[62] Section 27 of FIPPA requires that where a public body collects personal information directly from an individual—such as when ICBC takes photographs of citizens—the public body must ensure that the individual is told the purpose and legal authority for the collection. The notice must also include contact information for an employee within the public body who can answer questions.

[63] Notification allows the public to understand the purpose, nature and extent of collection of personal information. Without proper notification, the public is unable to ensure that their rights under FIPPA are preserved. Individuals unaware of the use of biometrics such as facial recognition, cannot object to or question the technology.

[64] ICBC advised that the purpose for the implementation of FR technology in November 2008 was to enhance the security of BCDLs and BCIDs by detecting and preventing fraudulent use or obtaining of these documents.

[65] ICBC provides some notification in the following two ways: (1) on the Driver Statement of Declaration provided with interim licenses and (2) on signage in some, but not all of its offices. The notices make no reference to the use of FR technology, nor to the use of the information for the purposes of preventing fraudulent use or obtaining of drivers' licences or BCIDs.

[66] I find that these notifications are inadequate because they fail to adequately describe the purposes for the collection of personal information and because the signage is not used in all offices. Further, the Driver Statement of Declaration fails to adequately describe the purposes for the collection and there is no equivalent statement signed by applicants for a BCID.

[34] Refer to smart meter requirement for better notification.

Recommendation #1:

I recommend that ICBC create a clear notification that includes a statement that facial recognition technology is in use for the purposes of preventing individuals from fraudulently obtaining drivers' licences or BCIDs as well as detecting and preventing their fraudulent use. The notification must also include notice of the legal authority for collecting the information and the title, business address and contact information of an employee who can answer the individual's questions about the collection.

At a minimum, the notifications should be provided as follows:

- post in all ICBC offices that serve the public;
- post on the ICBC website;
- mail to all drivers when they are notified of the need to renew their driver's licences;
- mail to all individuals when they are notified of the need to renew their BCIDs; and,
- include in all applications for new driver's licences or BCID cards.

Use of Personal Information

[67] Section 32 of FIPPA requires a public body to ensure that personal information in its custody or under its control is used only in accordance with the limits imposed under that section:

Use of personal information

32 A public body must ensure that personal information in its custody or under its control is used only

(a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34),

(b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or

(c) for a purpose for which that information may be disclosed to that public body under sections 33 to 36.

[68] ICBC states that it uses the digital images it collects under the authority of the *Motor Vehicle Act* and Voluntary Identification Card Regulation to create FR templates.

[69] ICBC states that the use of FR technology is for security purposes, that is, to prevent individuals from fraudulently obtaining drivers' licences or BCIDs and from their fraudulent use. ICBC argues that the specific language of the *Motor Vehicle Act* and the Voluntary Identification Card Regulation supports the conclusion that the original purpose for collecting photographic images when issuing drivers' licences BCIDs includes security purposes. ICBC points in particular to ss. 69 and 70 of the *Motor Vehicle Act*. They note that photo images were collected for the purposes of identification and that ICBC uses FR technology for the same purpose—to ensure individuals are accurately identified. Therefore ICBC concludes that the use is authorized under s. 32(a) of FIPPA since it is for the purpose for which the information was obtained.

[70] Section 69 of the *Motor Vehicle Act* provides that it is an offence for a person to apply for a driver's licence or identification card using fraudulent or altered records or false or misleading statements. Section 70 provides that it is an offence to possess an identification card or driver's licence that is fictitious or invalid. In order for these provisions to have effect, there must be some means for assessing the validity of identification provided by individuals which in turn suggests that ICBC, as the issuer of these two types of identification, has a responsibility to ensure the accuracy of these documents. Further, while s. 25(3) of the *Motor Vehicle Act* states that the purposes for this collection of photographic images are to determine an applicant's driving experience, driving skills, qualifications, fitness and ability to drive and operate any category of motor vehicle, it also provides that each driver must "identify himself or herself to the corporation's satisfaction."

[71] Reading these provisions as a whole, I am satisfied that the original purpose for the collection of photographic images of driver applicants includes security purposes. Therefore, I find that the use of photographic images through facial recognition to prevent fraudulent use or obtaining of driver's licences is authorized under s. 32(a) of FIPPA.

[72] Alternatively, I am also satisfied that if the use was not precisely for the original purpose, it was for a consistent purpose within the meaning of ss. 32(a) and 34 of FIPPA.

[73] For a secondary use to be consistent with the original purpose for collection, the secondary use must have a reasonable and direct connection to the original purpose for collection and must be necessary for performing the statutory duties of the public body or for operating a program or activity of the public body [FIPPA, ss. 32 and 34].

[74] For the reasons stated above, I am satisfied that the security purpose has a reasonable and direct connection to the original purposes enumerated in the *Motor Vehicle Act*. However, in order to satisfy the consistent purpose test, the use must also be "necessary".

[75] Former Commissioner Loukidelis provided an extensive review of the case law on the meaning of "necessary" in Order F07-10[35] paragraphs 37-46. Order F07-10 related to a complaint that a School Board was improperly collecting personal information in online assessments of applicants for teaching positions. With respect to the use of the word "necessary" in s. 26 of FIPPA he concludes,

> [19] A relevant part of the interpretive context of s. 26(c) and FIPPA overall is the reality that governments need personal information to do their work. They cannot provide services, confer benefits or regulate conduct without our personal information. For this reason, citizens may be compelled by law to give up their personal information or will disclose it to receive services or benefits and one cannot ignore the power of the state in relation to personal information collection in interpreting what is meant by "necessary" in s. 26(c).
>
> [20] The collection of personal information by state actors covered by FIPPA—including local public bodies such as the Board—will be reviewed in a searching manner and it is appropriate to hold them to a fairly rigorous standard of necessity while respecting the language of FIPPA. It is certainly not enough that personal information would be nice to have or because it could perhaps be of use some time in the future. Nor is it enough that it would be merely convenient to have the information.
>
> [21] At the same time, I am not prepared to accept, as the Complainants contend, that in all cases personal information should be found to be "necessary" only where it would be impossible to operate a program or carry on an activity without the personal information. There may be cases where personal information is "necessary" even where it is not indispensable in this sense. The assessment of whether personal information is "necessary" will be conducted in a searching and rigorous way. In assessing whether personal information is "necessary", one considers the sensitivity of the personal information, the particular purpose for the collection and the amount of personal information collected, assessed in light of the purpose for collection. In addition, FIPPA's privacy protection objective is also relevant in assessing necessity, noting that this statutory objective is consistent with the internationally recognized principle of limited collection.

[35] [2007] B.C.I.P.C.D. No. 10.

[76] As discussed previously, ICBC conducted a series of studies beginning in 1998 to evaluate the extent of fraudulent use of drivers' licences and BCIDs and the consequences of that fraudulent use. The most common reasons identified for the fraudulent use of drivers' licences and BCIDs were identified as:

- to avoid payment of past fines or debts and/or to avoid restrictions imposed by the previous driving-related convictions;
- to avoid taking the knowledge test or road test or both; and
- to acquire multiple drivers' licences or identification cards in order to commit fraud against ICBC and/or other agencies and organizations.

[77] At the time of the study, there were more than 3.5 million images in the driver database and the only way to compare images was to do a one-to-one comparison. That is, when an individual came in to renew his driver's licence, his old photograph could be retrieved and compared to the new photograph taken. There was no way to proactively determine if the individual had obtained other identification under a different name.

[78] ICBC also evaluated the liabilities it faced as a result of fraud and estimated the costs to the Corporation at $10.8 million per year and to other ministries at a further $80 million annually.

[79] The studies identified a number of strategies to attempt to reduce fraud other than implementing FR technology. ICBC reported that while it implemented most of these alternative strategies, none of these recommended strategies could stop the issuance of multiple IDs. ICBC then conducted tests to determine the effectiveness of FR technology and subsequently proceeded with implementation of the technology.

[80] I am satisfied, based on the extensive research conducted by ICBC, the implementation of a number of measures short of facial recognition and the testing of FR technology, that facial recognition software is necessary within the meaning of s. 34. Therefore, I am satisfied that the **use** of the facial recognition software for the purpose of detecting fraudulent activity is a consistent purpose within the meaning of s. 32(a) of FIPPA.

Protection of Personal Information

[81] **The Standard of Reasonableness**—Section 30 of FIPPA requires public bodies such as ICBC to make reasonable security arrangements to protect personal information in its custody or under its control. Section 30 reads as follows:

[82] A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

[83] Since 2006, we have published eleven investigation reports that have examined the meaning of "reasonable security arrangements".[36] We have consistently said that reasonableness is measured on an objective basis and while it does not mean perfect, depending on the situation, it may signify a high level of rigor.[37] More recently, I identified two circumstances where a high level of rigor was required.

[84] In Investigation Report F11-01, I examined the standard of reasonableness for an online platform. In determining that a high level of diligence was required I considered the nature of the known security risks to online platforms and the level of understanding of these risks by typical customers. I also took into account, the fact that government involvement increases the public's trust in the security and that the online environment is one of constant change that public bodies must respond and adapt to.

[85] More recently I examined the reasonableness of the security associated with the BC Hydro Smart Meter and Infrastructure Initiative in Investigation Report F11-03[38] and noted:

> [84] Given the increasing sophistication of hackers, all public bodies and organizations need to exercise due diligence in protecting the security of personal information in their custody or under their control. Security of systems requires ongoing vigilance. Public bodies must respond quickly to any identified privacy and security risks. Failure to do so would certainly not meet the requirements of FIPPA. However, reasonableness extends beyond a measure of responsiveness to identified risks. Public bodies must be proactive and implement ongoing monitoring and testing of the security of their systems. Public bodies also must ensure their policies are kept current and that their staff receives regular training.

[86] ICBC is the provincial Crown Corporation responsible for driver licensing, and vehicle licensing and registration. Due to government's involvement in verifying identity and licensing drivers, clients of ICBC have an increased level of trust and confidence in the security measures that ICBC has put in place to protect personal information. With this increased level of trust comes a corresponding increase in responsibility.

---

[36] We have in fact investigated or monitored almost 500 privacy breach reports since Jan. 2006.
[37] Investigation Report F11-01, [2011] B.C.I.P.C.D. No. 6, at paras. 30-34.
[38] Investigation Report F11-03, [2011] B.C.I.P.C.D. No. 43.

[87] Given that the FR system is capable of enrolling images from a variety of external sources—not just ICBC-created photographs—it would be possible for a rogue employee with access to the facial recognition system to enrol the photograph of say an ex-spouse's new partner. The facial recognition system could potentially identify the individual and provide access to date of birth, licence plate number, make and model of car and home address. Facial recognition is the ideal source for such clandestine tracking.

[88] As noted above, this technology is obscure and opaque. The average citizen will be unfamiliar with the technology and will not necessarily understand the privacy risks nor how to adequately protect themselves against them. Given these security risks, "reasonable" in the context of biometric systems such as ICBC's facial recognition system, requires a high level of diligence from the public body. I have applied this standard in our review and evaluation of ICBC's facial recognition system.

[89] **Safeguards**—In conducting this review, the investigation team interviewed ICBC staff responsible for the security, privacy and management of the FR system and also reviewed ICBC's documentation to assess the safeguards it currently has in place to protect personal information held within it. OIPC staff made three site visits to ICBC's offices to review the FR system and perform verifications of some of the controls in place surrounding the system.

[90] **Administrative Safeguards:**

Information security policies and procedures

ICBC has several policies that relate to customer privacy and information security. These include a corporate Code of Ethics, a Corporate Policy Guide and a series of Information Systems Security Policies and standards that cover topics such as risk assessment, governance, incident reporting and various technical controls both user and system based.

A message is presented to each user at the time of login with a reminder of the need to maintain the confidentiality of information stored within the system and the need to comply with ICBC's information security policies. The message includes a note advising the user that all activities on the system are logged and subject to review.

As a part of this investigation, we were able to review ICBC's policies and verify compliance through the review of risk assessment documents, incident reports and activity logs.

Information security training

ICBC employees and contractors are required to annually review and acknowledge ICBC's Code of Ethics as a condition of employment. New employees and contractors are required to complete a Privacy and Information Security Tutorial that includes scenario-based questions to help users understand ICBC's privacy and security requirements. As of October 2011, all personnel are required to undergo Privacy and Information Security training on an annual basis. ICBC's Privacy and FOI Department offers onsite privacy awareness training for ICBC departments and service providers.

Personnel clearances

All personnel who have access to the facial recognition systems have 'Secret' security clearance.[39]

[91] **Technical Safeguards**

Encryption of personal information

All of the facial images stored by ICBC are stored in an encrypted format and accessible only by authorized personnel. Information transmitted between the FR servers and workstations is encrypted from the starting point to the destination using Advanced Encryption Standard ("AES") with 128-bit encryption. The image database is encrypted with AES 256-bit encryption.

Access controls

Access to FR systems is managed centrally and controlled by restricting the workstations that are able to access this system and further restricting usage to users by their roles. Customer service personnel are able to enroll new images when a person renews or applies for a new driver's licence or BCID card. The ability to compare faces or to import photographs for comparison to those within the database is restricted to six fraud analysts and two supervisors within the FR Investigations Team.

Access controls exist at the network, application and database layers of the FR system.

[39] "Secret" security clearance is the type of screening required when the duties or tasks of a position necessitate access to classified information or assets. A "secret" level of security clearance is the fourth of five possible levels that consist of: non-sensitive, designated, confidential, secret and top secret. A secret clearance requires a background check that includes a background check, criminal record check and credit check.

Network security

All information related to FR is transmitted in an encrypted format over a private network that is actively monitored. Access to FR systems by authorized workstations is restricted using access control lists as well as user-level authentication. Differing security zones are separated by firewalls and other technical controls to prevent unauthorized access.

Malicious code controls

Protection against malicious code such as viruses and spyware is maintained and continually active on all workstations and servers.

Photo capture workstations

Dedicated photo capture workstations are used to enroll new clients and to renew the photo ID of existing clients. These workstations are managed and maintained by ICBC with up-to-date anti-virus software, current operating system patches and other controls as required by ICBC's information security standards. Automated locking mechanisms are in place on all photo capture workstations.

Facial recognition analysis workstations

ICBC's FR analysis workstations are located within access controlled security offices. Only Investigations personnel are permitted to enter the security offices unescorted.

The FR analysis workstations are maintained with up-to-date anti-virus software, current operating system patches and other controls as required by ICBC's information security standards. In addition, these workstations are configured to automatically lock after a very short period of inactivity. The department practice is for each user to manually lock his or her workstation prior to leaving the area.

Audit logging

Audit logging is in place for all workstations and servers that are a part of the FR system. Logs are created whenever a user accesses or changes a record. The logging system is configured to alert support personnel when key security events occur. Audit logs are retained indefinitely and archived on a monthly basis as disk space allows.

[92] **Physical Safeguards**

Data centre security

The data centre that houses the FR servers is a federally certified high security building.

[93] I am satisfied that ICBC has taken steps to ensure that the FR system is governed by a strong security framework and that all systems involved are adequately maintained. Security arrangements that are currently in place for the FR system meet the standard of reasonableness that is required by s. 30 of FIPPA.

Disclosure of Personal Information

[94] Public bodies are permitted to disclose personal information only as set out in ss. 33.1 and 33.2 of FIPPA.

[95] In the aftermath of the Stanley Cup riots, ICBC offered the use of its facial recognition technology to police for the purposes of identifying the alleged rioters. The proposed process was that police would supply photographs to ICBC. ICBC would then apply the FR software to those photographs and then compare the resulting FR templates to all of the templates stored in the ICBC database. ICBC would advise the police if a match was found and that a warrant or court order would be required before any disclosure of personal information occurred.

[96] As noted earlier, Vancouver Police did not follow up on ICBC's offer. However, during the course of our investigation we determined that even prior to the Stanley Cup riot, ICBC had received requests from police to identify individuals. Since January 2011, ICBC received 15 requests directly from police forces for assistance in identifying individuals. On at least one occasion, ICBC provided police with the possible identity of an individual based only on a police request under s. 33.2(i); no warrant or subpoena was required for the disclosure. Pending the outcome of this investigation, ICBC ceased accepting these requests from police forces and ceased disclosing information in response to these requests.

[97] ICBC discloses personal information to police in a variety of circumstances. The key disclosure at issue in this investigation is the disclosure of personal information following confirmation that ICBC's FR software has matched a photograph with a record in the drivers' licence database. The data elements that would typically be disclosed are the name, date of birth and address. Other elements could also be disclosed such as make and model of vehicle and licence plate number.

[98] ICBC relied on what was formerly s. 33.2 (b),[40] and s. 33.2(i) as authority for this disclosure. Section 33.2(i) permits disclosure of personal information to a public body or to a law enforcement agency to assist in a specific investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result.

[99] The essential requirements of this provision are that there be a specific investigation—at a minimum one would expect that the police have an open investigation file and are able to provide details regarding the scope of the investigation and file number. Further, it must be clear that the investigation is intended to lead to a law enforcement proceeding and is not simply information gathering, or background information. Where these requirements are met, ICBC would be authorized to disclose the minimum amount of information necessary to respond to the disclosure request. However, in responding to the request, ICBC must also satisfy the requirements of s. 32 of FIPPA with respect to use.

[100] Section 33.2(b) authorizes disclosure inside Canada in order to comply with a subpoena, warrant or order issued or made by a court, person or body in Canada with jurisdiction to compel the production of information. Effective November 14, 2011, this disclosure is now permitted pursuant to s. 33.1(1)(t) either inside or outside Canada.

[101] I agree with ICBC's position that it is authorized to disclose personal information in response to an order that satisfies the requirements of s. 33.1(1)(t). However, in responding to such a request, ICBC must also satisfy the requirements in FIPPA with respect to use of that personal information.

[102] **Use of facial recognition software to assist police**—When police make requests to ICBC, they supply a photograph from a source external to ICBC. Sometimes police have a potential name for the individual and sometimes they do not. All 15 requests received so far by ICBC from police were requests for the name of the individual in the supplied photograph.

[103] When an external image is provided to ICBC, the image is "enrolled" in the facial recognition system and a binary template is created if the image is of sufficient quality. That template is then compared against each of the 4.4 million templates within the ICBC system and potential matches are identified. To complete this process every template in the system must be used. The use involves the comparison of the binary codes and an evaluation of the match potential. Where the match score is high enough, the potential matches are

[40] This subsection was amended effective November 14, 2011. The disclosure for the purposes of law enforcement was previously authorized only inside Canada pursuant to s. 33.2(b) but is now authorized inside or outside Canada pursuant to s. 33.1(1)(t).

reviewed by human technicians who determine finally whether a match has in fact been found.

[104] Earlier I discussed the privacy concern known as 'function creep" where a system that holds data collected for one specific purpose is subsequently used for another unintended or unauthorized purpose.[41] It is of particular concern because the change in use usually happens without the knowledge or consent of the individual involved. Further, biometrics has the potential to become the technology of surveillance because, through the use of a biometric identifier, the ease with which surveillance through the use of data can be undertaken increases significantly.[42]

[105] The essential use rule in FIPPA is that personal information can only be used for the original purpose it was obtained. Any change in use is an exception to this basic rule and must be authorized in FIPPA. With the proliferation of new technologies, personal information collected for one purpose may be used to meet new and possibly unanticipated purposes with breathtaking speed and ease. If we are to maintain robust privacy rights great care must be taken in evaluating proposed changes in use. The language in FIPPA makes it clear that such changes in use are authorized in very specific and limited circumstances.

[106] ICBC cites s. 32(c) of FIPPA as authority for the use of the ICBC FR database to respond to requests from police:

> 32 A public body may use personal information in its custody or under its control only
>
> …
>
> (c) for a purpose for which that information may be disclosed to that public body under sections 33 to 36.

[107] ICBC points out that under s. 33, police may request personal information from other public bodies to assist in a specific investigation [s. 33.2(i)] or through the use of a subpoena, warrant or court order [s. 33.1(1)(t)]. Interestingly, when ICBC conducted a privacy impact assessment of the issues relating to proposed disclosures under s. 33.2(i), their privacy analyst determined that the use was not authorized under s. 32(c). ICBC advised that they obtained a further opinion from their legal department which disagreed with the conclusions of the privacy analyst.

[108] Like collection of personal information, the use of personal information by public bodies covered by FIPPA will be reviewed in a searching manner and it is

---

[41] OECD, Working Party on Information Security and Privacy, "Biometric-Based Technologies", 30 June 2004, DSTI/ICCP/REG(2003)2/FINAL at p. 12.
[42] OECD at p. 12.

appropriate to hold them to a rigorous standard of necessity while respecting the language of FIPPA.[43]

[109] Section 32(c) serves a very specific purpose. That is, it is intended to allow public bodies who are responding to valid disclosure requests to use information supplied by other public bodies to respond to those disclosure requests. It also permits the public body to use personal information in its custody or under its control **that is responsive to the disclosure request** for the purposes of responding to that request.

[110] In other words, the rule in FIPPA is that a public body may use information it holds to respond to a valid disclosure request. But the information it is permitted to use is limited to information responsive to the specific disclosure request. For example, if the police ask for the address of Bob K. Smith, ICBC can search its records for information relating to Bob K. Smith and can disclose Bob K. Smith's address. In other words, they can do a one-to-one comparison. ICBC can only look up Bob K. Smith in their records.

[111] What s. 32(c) does not permit is the use of every record in an entire database for the purposes of responding to a disclosure request about a single individual made pursuant to s. 33.2(i). Because ICBC is conducting a one-to-many comparison to respond to these police requests, it is using every one of its 4.4 million FR templates to compare against the template created for the police supplied photograph. In responding to requests to identify unknown individuals for police, ICBC is in effect changing the purpose for the entire database. It is not merely using one template within the database to respond to a police request. The whole database is involved.

[112] Use of the FR database to assist police could, however, be permitted were the police to obtain a subpoena, warrant or order from a court. In that case, the court could specifically require ICBC to use every record in its FR database to determine the identity of an individual. The use of the FR database for the purpose of complying with the subpoena, warrant or order would then be permitted pursuant to ss. 32(c) and 33.2(1)(t) of FIPPA.

[113] In my view, the requirement of a subpoena, warrant or order is appropriate because there is judicial oversight of the change in use of ICBC's database. Judicial oversight is necessary to ensure that any change in use of this magnitude is proportional to the public good served by the infringement on privacy rights of citizens.

[43] Former Commissioner Loukidelis noted a similarly standard with respect to collection of personal information in Order F07-10 at para. 48.

[114] Where a police force intends to ask for a subpoena, warrant or order, I recommend that ICBC provide the court with a detailed description of the process that ICBC must undertake when it is attempting to identify using its FR database. This will assist the court in understanding the nature and extent of the change in use that is being requested so that ICBC is specifically authorized to access all biometric records in the database for a police investigation.

[115] In the absence of a subpoena, warrant or order from a court, I find that the use of ICBC's FR software and database for the purposes of responding to disclosure requests from police is not authorized under FIPPA.

Recommendation #2:

ICBC should immediately cease using the FR database to identify individuals in images provided by the police, unless authorized by a subpoena, warrant or court order.

Part 4: Privacy Management Program

[116] Public bodies are accountable for how they manage personal information. Public bodies should be able to demonstrate to themselves, citizens and to this Office in the event of a complaint investigation or audit, that they have an effective, compliant, adaptable privacy program in place. A privacy management program is the total of all actions taken by a public body to protect the personal information in its custody and control.[44]

[117] In order to comply with the privacy rules set out in FIPPA, public bodies need to ensure that they are building privacy into their business practices from the start and before they launch new programs or services. A strong privacy management program will help to minimize their risks and mitigate the impact of any privacy breaches.

[118] There will be times when errors and mistakes are made. However, with a solid privacy management program, public bodies will be able to identify their weaknesses, strengthen their practices and potentially raise the protection of personal information that they hold to a higher level than the bare minimum needed to meet legislation requirements.

[44] Investigation Report F11-03, at para. 124.

[119] What are the elements of a privacy management program? Appendix B to this report is a description of the elements we expect to see in a robust privacy management program. We provided ICBC with this description and asked them to provide us with information relating to each of the elements.

➢ Organizational Commitment

[120] Privacy management programs begin with organizational commitment and program controls. Fundamentally, in order to be compliant and effective, a privacy-respectful culture needs to be cultivated. Senior management need to actively champion the privacy program. At a minimum, every public body should have a privacy officer.

[121] At the time of our investigation, ICBC's lead on privacy related matters is the Manager, Privacy and Freedom of Information. The Manager reports to a Vice-President who in turn is a member of the Executive Team. The results of this investigation indicate that the role of the Manager, Privacy and Freedom of Information as the "lead" on privacy related matters has not been adequately communicated throughout the organization. For example, there is no evidence that, prior to making the offer of FR technology to the Vancouver Police Department, the Manager of Privacy was consulted on whether or not that change in use would be compliant with FIPPA.

[122] Also, in July 2010, a Senior Information Officer completed a privacy impact assessment of the proposal to use ICBC's FR software to identify individuals from police surveillance photographs. The Senior Information Officer concluded that such use was not authorized under FIPPA. However, ICBC chose not to accept this conclusion.

[123] We were not provided with any documentation of the evaluation of why the original Privacy Impact Assessment ("PIA") was not accepted. No doubt, part of the problem, as discussed below, is that ICBC's assessment template is inadequate to properly evaluate the complex privacy issues associated with technology such as biometrics. We were provided with a requirements document dated September 2010 entitled, "Court Ordered Facial Recognition" that describes the process ICBC proposed following receipt of a court order. Based on these examples, it appears that there is insufficient privacy analysis in decisions around implementation of new technology.

[124] One way to rectify this is for the Manager, Privacy and Freedom of Information to have a higher profile within the organization, and a clear, wide mandate as the lead in all matters relating to privacy. The Manager also needs to be able to communicate well with Senior Executive and influence decision-making processes in order to foster a culture of privacy within ICBC.

Recommendation #3:

I recommend that ICBC establish accountability and leadership for privacy within the corporation to ensure that privacy is taken into account in decision-making processes at the Senior Executive level. This would help to foster a culture of privacy within ICBC.

➢ Privacy Program Controls

[125] Privacy tools or program controls are another essential element of a privacy management program. These include a personal information inventory, privacy policies, risk assessment tools and training and education requirements.

[126] ICBC has implemented a comprehensive set of information security policies, principles and standards that address key components of a security architecture including risk assessment, system patching, perimeter security, mobile device security, incident reporting and the maintenance of user accounts. There is an established governance framework for information security. A cross-functional team reviews and updates information security policies and standards as necessary. Security threat risk assessments are conducted on new systems, as well as those undergoing a significant change, to identify risks and determine the necessary controls to mitigate those risks.

[127] However, ICBC's privacy impact assessments are inadequate, particularly for an organization that manages so much sensitive personal information. The implementation of FR technology highlights these inadequacies. The initial assessment of the privacy issues associated with the use of biometrics was completed by external legal counsel in June 1999. At that time, the issue was whether ICBC could conduct a pilot using FR technology for the purpose of fraud detection and prevention. In July 1999, ICBC conducted a privacy impact assessment using ICBC's PIA form. Both assessments concluded that ICBC could implement FR technology for the purposes of fraud detection in compliance with FIPPA.

[128] In February 2006, ICBC conducted another privacy review that consisted of a one-page document that discussed privacy issues associated with facial recognition. This was followed by a two-page discussion document dated September 6, 2007, that provided slightly more detail regarding what the proposed FR technology would entail. The conclusion reached in both documents was that nothing in the proposal offended any provision of FIPPA.

[129] ICBC implemented FR technology in November, 2008. No comprehensive privacy impact assessment was completed on the technology that was purchased and implemented in November 2008.

[130] Privacy impact assessments are key privacy controls essential to ensuring that new projects and programs are designed and implemented in a manner consistent with legal requirements. They help to identify privacy and security risks early on, improve the design and implementation of projects and allow organizations to plan risk mitigation strategies. ICBC's documents briefly list basic privacy rules in FIPPA and state conclusions without any detailed analysis of how the conclusions were reached. The documents provide no description of the proposed technology or of the data elements collected, used or disclosed, no information flow analysis, there is no discussion of the proposed security and no risk assessment or mitigation plans discussed. Without detailed description of the proposed technology and the proposed implementation processes, it is impossible to evaluate the conclusions stated in these documents.

[131] ICBC provided us with some policy documentation regarding when and how a privacy impact assessment needs to be completed. In our view, the policies are not adequate as they do not clearly mandate the completion of privacy impact assessments, fail to require review and update of PIAs (an evergreen process) and further, ICBC does not have an adequate privacy impact assessment template to evaluate the complex privacy issues for projects such as facial recognition.

Recommendation #4:

ICBC should develop, implement and communicate a privacy impact assessment policy that sets out parameters for when and how a privacy impact assessment must be completed. The policy should provide that PIAs must be regularly reviewed and that technology projects should go through phases of reviews at the conceptual, design and implementation phases. Finally the PIA policy should include a detailed template that assists employees to properly identify and analyze privacy risks.

[132] During this investigation, ICBC advised us that they have initiated a comprehensive review of its PIA process to ensure that PIAs are completed when necessary and are sufficiently comprehensive so that the complexity of proposed initiatives is properly analyzed and the privacy risks are addressed.

➢ Ongoing Assessment and Revision

[133] The second essential element of a privacy management program is ongoing maintenance work which consists of performance planning for the privacy office, monitoring various elements and updating policies, personal information inventories and notices.

[134] ICBC's Privacy and Freedom of Information Department ("Department") has a performance plan for 2011. The plan appears to be adequate in terms of ensuring that PIAs are completed and that training is delivered. There is no mention of a policy review schedule. Policy review may be the responsibility of the Information Security and Privacy Committee. The Committee's Charter, dated July 2009, states that its purpose is to provide governance oversight to information security and privacy policies. However, the Committee has not met since December 2010. ICBC says that the work has been carried out informally and that the Committee may be replaced by a new Data Governance Office.

[135] Policies should be reviewed on both a regular basis and on an ad hoc basis as issues arise. Privacy policies can easily become stale or irrelevant as business processes change and as technology, such as biometrics, are implemented.

Recommendation #5:

ICBC should assign privacy policy review responsibilities and ensure that a schedule to review all privacy policies is developed and implemented.

[136] Another element of ongoing assessment is the need to monitor notifications to ensure that they are accurate and up to date. As discussed earlier, the notices posted in ICBC's driver licensing facilities fail to adequately describe the purposes for the collection of personal information and because the signage is not used in all offices. Further, the Driver Statement of Declaration fails to adequately describe the purposes for the collection and there is no equivalent statement signed by applicants for a BCID. As a result, I have recommended improvements in notifications.

Part 5: Conclusions

[137] Our ability to control information about ourselves lies at the heart of the right to privacy in FIPPA. Citizens are entitled to know what information is being collected about them and why. Public bodies must limit the use of personal information to the purposes originally identified unless FIPPA permits a change in use. Facial recognition challenges our understanding of the rules set out in FIPPA. It is a technology that has the potential to significantly impact our right to privacy.

[138] Through this investigation, I determined that ICBC adopted and implemented a technical solution that was necessary to address the problem it identified—fraudulent acquisition and use of drivers' licences and BCIDs. However, ICBC did not fully satisfy all of the legal requirements when it implemented facial recognition. Specifically, it did not provide adequate notice to citizens. Further, I identified three key areas of ICBC's privacy management program that require improvement.

[139] With respect to ICBC's offer to assist police in their investigation of the Vancouver riot, I determined that the change in use of ICBC's facial recognition database was not authorized under FIPPA. ICBC must receive a warrant, subpoena or court order before it uses its FR software to assist police with their investigations.

[140] My findings and recommendations are summarized below:

1. The measurements taken and the unique biometric template created by applying the algorithm to the measurements is personal information within the meaning of FIPPA.

2. ICBC has the express statutory authority to collect digital images for the purposes of issuing BCIDs and BCDLs.

3. The manipulation of existing data to create facial recognition templates does not result in the collection of new personal information but does involve a new use of personal information that must satisfy the requirements of s. 32 of FIPPA.

4. The current notification regarding the purposes for collection of personal information by ICBC when photographs are taken is inadequate because it fails to adequately describe the purposes for the collection of personal information and because the signage is not used in all offices. Further, the Driver Statement of Declaration fails to adequately describe the purposes for the collection and there is no equivalent statement signed by applicants for a BCID.

5. The use of photographic images through facial recognition to prevent fraudulent use or obtaining of driver's licences is authorized under s. 32(a) of FIPPA.

6. The security arrangements that are currently in place for the facial recognition system meet the standard of reasonableness that is required by s. 30 of FIPPA.

7. In the absence of a subpoena, warrant or order from a court, the use of ICBC's FR software and database for the purposes of responding to disclosure requests from police is not authorized under FIPPA.

RECOMMENDATIONS

Recommendation #1: I recommend that ICBC create a clear notification that includes a statement that facial recognition technology is in use for the purposes of preventing individuals from fraudulently obtaining drivers' licences or BCIDs as well as detecting and preventing their fraudulent use. The notification must also include notice of the legal authority for collecting the information and the title, business address and contact information of an employee who can answer the individual's questions about the collection.

At a minimum, the notifications should be provided as follows:

- post in all ICBC offices that serve the public;
- post on the ICBC website;
- mail to all drivers when they are notified of the need to renew their driver's licences;
- mail to all individuals when they are notified of the need to renew their BCIDs; and,
- include in all applications for new driver's licences or BCID cards.

Recommendation #2: ICBC should immediately cease using the FR database to identify individuals in images provided by the police, unless authorized by a subpoena, warrant or court order.

Recommendation #3: I recommend that ICBC establish accountability and leadership for privacy within the corporation to ensure that privacy is taken into account in decision-making processes at the Senior Executive level. This would help to foster a culture of privacy within ICBC.

Recommendation #4: ICBC should develop, implement and communicate a privacy impact assessment policy that sets out parameters for when and how a privacy impact assessment must be completed. The policy should provide that PIAs must be regularly reviewed and that technology projects should go through phases of reviews at the conceptual, design and implementation phases. Finally the PIA policy should include a detailed template that assists employees to properly identify and analyze privacy risks.

Recommendation #5: ICBC should assign privacy policy review responsibilities and ensure that a schedule to review all privacy policies is developed and implemented.

ACKNOWLEDGMENTS

[141] ICBC cooperated fully with our investigation and has agreed to implement each of the recommendations.

[142] Catherine Tully, Assistant Commissioner and Angela Swan, Technical Investigator, conducted this investigation and prepared this report with assistance from Helen Morrison, Senior Policy Analyst.

February 16, 2012

ORIGINAL SIGNED BY

_____
Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

OIPC File No. F11-45996

APPENDIX 'A'
RELEVANT STATUTORY PROVISIONS

Motor Vehicle Act

25(3) For the purpose of determining an applicant's driving experience, driving skills, qualifications, fitness and ability to drive and operate any category of motor vehicle designated for that class of driver's licence for which the application is made, the applicant must

…

(d) submit to having his or her picture taken

82(1) If a record is kept by the Insurance Corporation of British Columbia, the director or the superintendent under this Act, the corporation, director or superintendent, as the case may be, may

…

(b) have the record or its contents stored in electronic format,

…

(d) keep the record or its contents in any other prescribed manner.

82(2) If information from a record to be kept by the Insurance Corporation of British Columbia, the director or the superintendent is converted into another format under subsection (1), the corporation, director or superintendent, as the case may be, may destroy the paper format of the record and the information, in the format into which it has been converted, is deemed to be the record so converted.

Voluntary Identification Card Regulation, BC Reg. 465/88

3(1) The Insurance Corporation of British Columbia must issue a numbered identification card in a form established by the corporation to an applicant who has

…

(b) had his or her picture taken digitally or electronically…

APPENDIX 'B'
PRIVACY MANAGEMENT PROGRAM – THE ESSENTIAL ELEMENTS

BUILDING BLOCKS
1. Organizational Commitment
Chief Privacy Officer • Role exists and is defined • Part of the executive team • Reporting relationship supports the ability of the CPO to influence decisions • Role and responsibilities are communicated throughout the organization • Reports on the implementation of the privacy management program **Information and Privacy Office** • Role is defined and resources are adequate • Organizational structure supports the ability of the IPO staff to influence decisions in support of access and privacy
2. Privacy Tools/Program Controls
(1) Personal Information Inventory o What personal information is your public body or organization collecting, using & disclosing? o Why – i.e. what are your authorities? o What security do you have in place? **(2) Essential privacy policies** o Privacy breach management policy o Security policies: systems security policy, travelling with personal information policy, physical security policy including a garbage and recycling policy o Role based access policy o Guidelines on the collection, use and disclosure of personal information o Retention and disposal policy o **Other policies:** Privacy accountability policy, Training policy, Research, Third Party contracting, PIAs, Information classification, Risk assessment, Monitoring and auditing, Business continuity, Change control **(3) Privacy Impact Assessments & Security Threat and Risk Assessments** o Initial PIA process in place to ensure assessments are completed at the conception, design and implementation phases of all new projects o Evergreen PIA process in place o Conduct STRA's on new systems to ensure reasonable security **(4) Privacy Protection Schedules** o Included in all contracts involving personal information **(5) Training & Education** o Mandatory for all staff and service providers with access to personal information
3. Reporting Structure
• Clearly defined in terms of overall compliance • Employees aware of reporting structure for complaints and breaches • Reflected in policies and procedures

CONTINUOUS IMPROVEMENT

1. Plan

- Information and Privacy Office has annual performance plan – will likely include privacy audit schedule, training schedule, policy review schedule and performance measures.

2. Monitor

1. **New rules**, expectations and best practices.

2. **Internal practices** for new processes or changes that collect, use or disclose personal information. Have a regular audit cycle that includes evaluation of compliance with privacy laws, policies and procedures.

3. **Contractor compliance** using:
   a. audits
   b. review of privacy training & privacy policies
   c. regular updates of confidentiality agreements

4. **Public complaints and disputes** to identify areas of risk, training needs, policy needs.

5. **Privacy Awareness and Training** to ensure completion by all staff on a regular basis, keep training up to date and ensure confidentiality agreements are signed on an annual basis

3. Maintain

1. **Privacy policies, procedures and practices** are monitored, assessed and adapted
   - On an as-needed basis if there is a legislative or system change or to reflect breach investigation recommendations
   - On a regular cycle
   - Changes are communicated to staff

2. **Personal information inventory**
   - Maintain the inventory – identify & evaluate new collections and disclosures

3. **Notices**
   - Ensure notices are accurate and up to date

4. **Effective Security System**
   - Test security to ensure it's reliable
   - Audit

5. **Effective Breach Management System**
   - Conduct post incident reviews to evaluate effectiveness of breach management system
   - Adapt breach management system to implement best practices

Appendix 'C'
FACIAL RECOGNITION TECHNOLOGY - A BIBLIOGRAPHY

Privacy experts, particularly in Europe and North America have identified a number of significant privacy concerns associated with FR technology described briefly below. A list of articles discussing ethical and privacy concerns relating to biometrics generally and facial recognition in particular are also listed below.

Interoperability: Until fairly recently the absence of standards of interoperability at the international level meant that biometric systems, for the most part were not compatible. However, recent developments in international standards now mean that biometric solutions are growing more compatible or interoperable. Interoperability means that biometrics collected by one organization for one purpose can now be used by another organization for a different purpose.

Over collection/secondary information: Biometrics has the potential to collect information about race and ethnic origin. Various facial features and skin tone are most associated with particular racial or ethnic origins. So while the organization may not intend to collect information about racial or ethnic origin, they may nevertheless be collecting such information without authority.

Clandestine tracking: Clandestine tracking refers to the concern that the creation of a large database of information on individuals may enable a government to secretly monitor the activities of individuals.

Security risks: The growth in the use of biometrics systems and the likely expansion of agencies having access to individual's biometric information – both government bodies and private organizations raises concerns regarding the security of the information and the potential for misuse.

Accuracy: Accuracy is a concern in two ways. First, there may be an assumption by organizations that have implemented facial recognition that the system is accurate and a match is reliable. The consequences that flow from a match could include deportation or criminal charges. In addition, there are some known inaccuracies with facial recognition including the fact that facial imaging has proven to be less accurate as the photo ages. Organizations must have in place a means to re-evaluate the accuracy of any match identified through the FR software.

Ajana "Recombinant Identities: Biometrics and Narrative Bioethics"

Alterman, "A piece of yourself": Ethical issues of biometric identification" (2003)

Article 29 Data Protection Working Party "WP 80 – Working document on biometrics" (2003)

Introna, Lucas, Disclosive Ethics and information technology: disclosing facial recognition systems, Ethics and Information Technology (2005)7:75-86

Lyon, “Biometrics, Identification and Surveillance” (2008)

Mordini & Massari, “Body, Biometrics and Identity” (2008)

Mordini & Petrini, “*Ethical and social implications of biometric identification technology*” Ethical and Social Implications of Biometric & Identification Technology Ann 1st Super Sanita vol. 43 at p. 5

OECD Working Party on Information Security and Privacy, “Biometric Based Technology” (2004)

Redpath, “*Biometrics and international migration*” Ethical and Social Implications of Biometric & Identification Technology Ann 1st Super Sanita vol. 43 at 27.

Facial Recognition and the Limits of Privacy Law – Harvard Law (2007)

Appendix 'D'
GLOSSARY OF TERMS

BCID	British Columbia Identification Cards BCIDs are identification cards intended for non-drivers who require a legal piece of identification. BCIDs are typically used in any situation where a driver's licence would be used for identification. Anyone 12 years or older can apply for a BCID
Biometrics	"Biometrics" is literally, the measurement of life. It refers to the technology of measuring, analyzing and processing the digital representations of unique biological data and behavioral traits such as fingerprints, eye retinas, irises, voice and facial patterns, gaits, body odours and hand geometry
DL	Driver's licences issued by ICBC.
FR	Facial recognition
FR template	Facial recognition template—a unique number created through the use of facial recognition software. The number is made up of a long series of zeros and ones (binary code) and is unique to each photograph.
Fake ID	Fake identification is identification using replica and home-made versions of official documents.
False ID	False identification refers to legitimate identification falsely obtained. That is, individuals obtain identification directly from federal and provincial organizations under a false name.
IMPACT	IMPACT is a joint law enforcement initiative funded by ICBC. It is known mainly for its bait car program which involves setting up cars with hidden cameras used to catch thieves as they attempt to steal the bait car.
One-to-one comparison (1:1)	When the new measured biometric is compared against one known to come from the same individual. This measurement answers the question, "Is this person who s/he claims to be".
One-to-many comparison (1:N)	When the new measured biometric is compared against every biometric stored in the database. It can answer the question, "Who is this person?"