INVESTIGATION REPORT 23-02

Canadian Tire Associate Dealers' use of facial recognition technology

APRIL 2023
CANLII CITE: 2023 BCIPC 17
QUICKLAW CITE: [2023] B.C.I.P.C.D. NO. 17

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

Imagine a world where, before entering your favourite retail store, you are asked to place your fingers on a black inkpad to have your prints taken.

The greeter explains the store only wants to make sure your prints don't match an alleged shoplifter, or a customer who suspiciously uses the returns counter too often.

In practical terms, that is what happens when retailers or other organizations deploy modern technologies to scan your body features before you enter their establishments -- albeit in a more "frictionless" and surreptitious way.

Today's software systems powered by artificial intelligence (AI) have enabled organizations to measure with precision our physical attributes – from the way we walk to the shape of our irises to old-fashioned fingerprints.

The impact of recording and digitizing our unique human characteristics, often referred to as "biometrics", is profound.

In this report, we focus specifically on the use of "facial recognition technology," known as FRT, in the retail sector. This technology works by capturing a person's facial image, usually by still camera or video, and then creating an exact mathematical rendering of those facial features and proportions. This rendering, reduced to a template, is then compared to a database of stored facial biometrics representing a certain population.

Each human face is unique, and for that reason a template generated from it by an FRT system is a highly sensitive personal identifier.

There are appropriate uses for FRT in certain circumstances, such as a credential to unlock your phone, where your biometric resides on your device and is within your control.

But FRT systems can do much more than making simple tasks more efficient. They can now gather and compare unique facial identifiers on an expanded scale. This poses a particular challenge and danger to society when those images are inappropriately collected, used, mismanaged, or treated without due restraint and oversight. Therefore, organizations seeking to routinely deploy this technology at scale, especially in publicly accessible places, should be prepared to demonstrate a highly compelling case to do so.

Why?

First, FRT can get things wrong, incorrectly matching a captured face with a comparative database. That is especially true when it comes to people of colour and minorities. Those false matches can damage reputations, inflict psychological stress, and even lead to wrongful

detainment or imprisonment. The recent case of Randal Reid, an African American man living in Atlanta, Georgia is an example[1]. Mr. Reid was driving to his mother's house when four police vehicles pulled him over on a suspicion that he committed theft in another state. That state extradited and detained him for six days before discovering it had the wrong man. Mr. Reid's image had been collected without his consent by a company called Clearview AI and compared to an image of the suspect. The FRT system incorrectly matched the two, leading to Mr. Reid's arrest. Many days and many thousands of dollars in legal fees later, Mr. Reid was allowed to go home.

Second, the comparative database itself might be discriminatory, and arbitrarily or improperly collected. Mr. Reid's image was collected without his knowledge, which, if it occurred in Canada, would have constituted a violation of our country's privacy laws.[2] That same database might also contain people never found to have committed a wrongdoing, only suspected by someone of doing so. Or the comparative database might just be people an organization simply didn't like - as was the recent case of Madison Square Garden's banning of members of a law firm involved in litigation with them.[3]

Third, we know that databases storing troves of sensitive biometric data become high-value targets for cybercrime. Whether accidental or intentional, biometric data breaches can exacerbate acts of stalking, identity theft, and financial fraud. The stakes are high because a person's digital facial print, unlike a computer password, cannot be changed if it is hacked or stolen.

Finally, a pervasive spread of biometric surveillance infringes on every citizen's right of privacy and robs the public of its right to anonymity. It should not be the case in a free and democratic society that simply by walking in a public space, or through a given entrance way, a person hands over their highly detailed physical measurements.

In the report that follows I find that the application of biometric surveillance, in the circumstances outlined, do not accord with BC's privacy law. Invasive surveillance of untold numbers of people was a disproportionate response to the challenges faced by the stores. In my view, retailers would have to go some way to legally justify the collection of biometrics from everyone who enters their premises. As a democratic society, we must proceed with caution, or not at all in many cases, when it comes to FRT.

---

[1] *Thousands of dollar for something I didn't do* https://www.nytimes.com/2023/03/31/technology/facial-recognition-false-arrests.html

[2] *Report of Findings: Joint investigation of Clearview AI, Inc., by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information and Privacy Commissioner of Alberta*: https://www.oipc.bc.ca/investigation-reports/3505

[3] *Madison Square Garden uses facial recognition to ban its owner's enemies* https://www.nytimes.com/2022/12/22/nyregion/madison-square-garden-facial-recognition.html

EXECUTIVE SUMMARY

The Office of the Information and Privacy Commissioner for British Columbia (OIPC) investigated the use of facial recognition technology (FRT) by four Canadian Tire stores (the stores) located in British Columbia.

Facial biometrics are particularly sensitive, distinctive, and immutable pieces of personal information.

For approximately three years, the investigated stores used FRT for the stated purposes of loss prevention and protecting staff and customers. Each of the involved stores promptly removed their FRT systems when they were notified of the OIPC's investigation.

The Commissioner determined that continuing the investigation would benefit the retail sector, other businesses, and lawmakers. The OIPC collected relevant documents and conducted interviews with store managers and vendors of the FRT systems. The OIPC assessed whether the stores notified and received consent from customers regarding the use of FRT, and whether the stated purposes for collection were reasonable.

The stores used FRT systems developed by AxxonSoft and FaceFirst. The systems collected facial images or videos of individuals entering the stores, created biometric templates from those faces, and compared these to a database of previously collected photos and biometric templates representing persons of interest who had allegedly been involved in incidents at Canadian Tire stores in the same region.

The investigation showed that the stores did not adequately notify customers and did not obtain consent for the collection of personal information using FRT.

Even if the stores had obtained consent, which they failed to do, they were still required to demonstrate a reasonable purpose for collection and use. The investigation found that they did not do so. Factors in that determination included the amount and sensitivity of the personal information collected, the limited likelihood of achieving the purposes for collection, and the availability of less-intrusive options.

This report makes three recommendations.

1. The stores should create and maintain robust privacy management programs that will better equip the stores for current and future decisions around managing personal information.
2. The BC Government should regulate the sale or installation of technologies that capture biometric information.

3. The BC Government should amend the *Personal Information Protection Act* to create additional obligations for organizations that collect, use, or disclose biometric information, including requiring notification to the OIPC.

1 BACKGROUND

Every human face is unique. Facial recognition technology captures that uniqueness through a series of facial measurements that create a precise rendering of who we are as individuals. For this reason, those renderings are highly sensitive personal information that cannot be collected in British Columbia, except in very limited circumstances.[4]

To date, 130 of the world's data protection and privacy authorities have expressed significant concerns about FRT.[5] The Global Privacy Assembly emphasized the importance of having a lawful basis prior to FRT applications, as well as evidence that biometric collection is reasonable, necessary, and proportional. This international body has emphasized the need for organizations to protect human rights, be transparent and accountable, and to establish strong data protections.

Legislators and policy makers in democracies around the globe have banned or significantly restricted certain uses of biometric technologies, including FRT.[6] When those uses are permitted, the technology is often reserved for law-enforcement agencies, who have broad collection authority. Even when operating exclusively in the hands of law enforcement, FRT is often restricted to limited circumstances, requires diligent security measures, and is subject to strict constitutional limits.

With this backdrop in mind, and in light of media reports[7] about well-known Canadian retailers employing FRT, the Information and Privacy Commissioner sought to assess the prevalence and application of FRT in BC's retail sector.

---

[4] OIPC Order P21-08. BCIPC 73. https://www.oipc.bc.ca/orders/3610.

[5] Global Privacy Assembly, October 2022. Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology. https://globalprivacyassembly.org/wp-content/uploads/2022/11/15.1.c.Resolution-on-Principles-and-Expectations-for-the-Appropriate-Use-of-Personal-Information-in-Facial-Recognition-Technolog.pdf

[6] See, for example: The Illinois *Biometric Information Privacy Act* (https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57), the European Union's proposed Artificial Intelligence Act (https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206), Canada's proposed Artificial Intelligence and Data Act (https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading), and Québec's *Bill 64—An Act to modernize legislative provisions as regards the protection of personal information* (https://www.canlii.org/en/qc/laws/astat/sq-2021-c-25/latest/sq-2021-c-25.html.

[7] For example: January 4, 2021, https://ccla.org/wp-content/uploads/2021/07/Interim-Report-Compiled-BM.pdf; January 23, 2021, https://globalnews.ca/news/7588121/facial-recognition-canada-rights/; February 21, 2019, https://winnipeg.ctvnews.ca/from-facial-recognition-to-extra-staff-high-and-low-tech-tools-used-to-combat-shoplifting-in-winnipeg-1.4307648.

The OIPC surveyed 13 of the province's largest retailers (including grocery, clothing, electronics, home goods, and hardware stores): 12 responded that they did not use FRT. The remaining retailer, Canadian Tire Corporation, requested that the OIPC contact their 55 independently owned Associate Dealer stores in the province. In the result, 12 stores reported using FRT.

Based on these 12 responses, the Commissioner exercised his authority under s. 36(1)(a) of the *Personal Information Protection Act* to investigate a sample of those responses. The four BC Canadian Tire Associate Dealers (the stores) selected represent three regions in BC: Lower Mainland, Vancouver Island, and the Interior.

2 METHODOLOGY

2.1 Issues for investigation

The OIPC began this investigation by asking whether the selected stores:

1. Were **required to obtain consent** for the collection, use, or disclosure of personal information, as per s. 6 of PIPA.
2. **Obtained consent** for the collection, use, or disclosure of personal information, as per s. 7 of PIPA.
3. **Provided notification** for the collection, use, or disclosure of personal information, as per s. 10 of PIPA.
4. Collected and used personal information for **appropriate purposes**, as per ss. 11 and 14 of PIPA.

2.2 Investigative methods

The OIPC undertook this investigation using the following methods:

1. **Reviewing written submissions** from the stores to ascertain:
    a. workings of their surveillance systems;
    b. purposes for collecting and using personal information via FRT;
    c. the period during which FRT was employed;
    d. the type of FRT software or products; and
    e. how facial biometrics were used.
2. **Reviewing stores' internal documents**, such as policies, contracts, and other written materials pertaining to video surveillance or FRT.
3. **Reviewing notifications or signage** pertaining to video surveillance or FRT.

4. **Conducting interviews** with store management (i.e. Associate Dealers, and IT or security managers) and, separately, with third-party service providers.
5. **Discussing regulation** of biometric technologies and vendors with Security Programs Division, Ministry of Public Safety & Solicitor General, BC Government.

A few weeks after they received the OIPC's November 16, 2021 notice of investigation, the stores removed hardware associated with FRT, wiped the servers in their custody and control, and returned equipment to the third-party vendors that supplied the technology.[8]

Even though the stores dismantled their FRT systems, the OIPC continued the investigation. The Commissioner considered a robust and public assessment of issues of notification and consent, and whether the purposes for collection were reasonable.

3 PERSONAL INFORMATION PROTECTION ACT (PIPA)

PIPA governs how organizations collect, use, and disclose personal information. PIPA requires organizations to process personal information in a manner that recognizes both the right of individuals to protect their personal information, and the legal obligation to only process personal information for purposes that a reasonable person would consider appropriate in the circumstances. Organizations maintain responsibility for compliance with PIPA, even when contracting out products or services.

Specifically, PIPA requires organizations to:

- be responsible for personal information under their control and ensure compliance with PIPA – s. 4;
- develop and follow policies and practices that demonstrate compliance with PIPA – s. 5;
- collect, use, or disclose personal information only with the consent of the individual or when PIPA permits these activities without consent – ss. 6-8 and s. 12;
- inform individuals about the purpose for collecting personal information at or before the time of collecting the information directly from them – s. 10; and
- collect, use, or disclose personal information, with or without consent, only for purposes that a reasonable person would consider appropriate – ss. 11, 14, and 17.

[8] The remaining eight stores that were not selected for investigation confirmed they also removed the systems shortly after the investigation was initiated.

4 OVERVIEW OF FRT SYSTEMS

Like many retailers, each of the four stores included in this investigation employ an intricate video surveillance system that covers entrances and exits, checkouts and returns, store parking lots, retail floors or service areas, and various offices. These video surveillance systems run around the clock, every day, to aid in preventing shoplifting, vandalism, or harassment and assault.

In 2018, three of the stores went further and implemented FRT systems – which included computer servers, software, and as many as seven motion-activated, high-definition FRT cameras at store entrances. The fourth store added the same technology in 2019.

According to each store involved in this investigation, FRT was implemented at the discretion of the individual store managers. The stores advised:

> There is no [corporate] mandate for dealers to install FRT or surveillance technology. …any use of FRT is at the discretion of the individual dealer and such technology would not be managed or supported except as arranged by the dealer. Canadian Tire Corporation has no access to any dealer FRT systems or data.[9]

Three of the stores used FaceFirst as their FRT system, installed by SilverPoint Systems (SilverPoint); one store used AxxonSoft, installed by SEQ Security Surveillance Services Inc. (SEQ), which included a standard FRT system, as well as a Returns Desk Verification System.[10]

Both systems generally operated by capturing images or videos of any person entering the stores, as they passed into view of FRT cameras. Visitors included customers, staff, delivery personnel, contractors, and others who may have entered the store (including minors).

Software then mapped facial coordinates from the images or videos, creating a biometric template of each unique face. The systems would then compare a newly arrived visitor's facial biometrics to others stored in a database of previously flagged "Persons of Interest." These individuals had been allegedly involved in incidents of theft, vandalism, harassment, or assault.

When a new visitor's facial biometrics matched an existing biometric record in the database, the FRT system sent an automatic alert to store management and security staff by email or directly through an FRT application on a mobile device. Alerts contained the newly captured image or video that triggered the match, and a copy of the previously collected image from the Persons of Interest database, along with any comments or details related to the prior incident(s). Store managers reported that these alerts were considered advisory until management or security personnel verified a match in person.

---

[9] Written submissions received from the store management on December 6, 2021.

[10] The Returns Desk Verification System is a fraud prevention system that called up images of individuals from their entry into the store, so staff could verify whether they were carrying the product they attempted to return.

Store management reported that after a positive match was verified, the nature of the prior incident allegedly involving the individual helped determine a course of action. If a prior incident included violence, management or security staff would escort the individual from the store. If the prior incident involved theft, management may have chosen to surveil or remove the person in question.

Store managers and the FRT vendors (SilverPoint and SEQ) reported that when the systems did not generate a match, recorded images and videos were stored in a "Visitor" database and overwritten (i.e., erased) after 30 to 60 days.[11] In contrast, when the systems did generate a match, images and facial biometrics were manually uploaded and stored in the Persons of Interest database for a longer period: two years in the FaceFirst system and, indefinitely in AxxonSoft, until manually deleted.

While serving the same overall function of facial recognition, the two systems were designed and operated in different ways – each is described below.

FaceFirst

According to store managers and SilverPoint personnel, each of the three stores' installation of the FaceFirst system consisted of one onsite-server computer connected to a central-database server managed by SilverPoint. The central-database server held a master copy of the Persons of Interest database, from which a copy was distributed to each of the stores' onsite servers.

Silverpoint reported that the central server, and an associated email server, which distributed alerts, were held at secure data centres in Canada. Both SilverPoint and the FaceFirst company had remote access to all central and local servers. Store managers and staff accessed an FRT application via web browsers. They received alerts through email inboxes (one per store) or through a mobile version of the FaceFirst application.

The FaceFirst systems captured a still image of each visitor to the stores and used those images to create facial biometrics that were then compared against biometrics stored in the Persons of Interest database. According to SilverPoint, new images that did not produce matches were kept in the Visitor database for 30 days, then deleted. Reportedly, associated biometrics of visitors were not retained.

When an incident occurred involving a specific individual, store managers or security staff manually entered that individual's personal information into the Persons of Interest database. From a limited series of drop-down lists, store personnel would select descriptors about the person of interest (for example, physical descriptions such as tattoos or scars), the nature of the incident, and the outcome or action taken. Entries also included facial images collected upon entry and facial biometrics generated within the system for comparison. SilverPoint reported

[11] The variance in time for the overwriting process to occur was based on the size limit specified for the database and the amount of foot traffic at the store.

that information logged in the Persons of Interest database was kept for two years and then automatically purged.

The FaceFirst system provided for the sharing of facial images and facial biometrics between stores. Each store could have used the shared database server to access the central Persons of Interest database, or used a non-shared server, in which case a comparison database would be built from persons of interest identified only at that location. According to SilverPoint, all stores chose to implement the shared-server option. Store servers (connected to the central database) sent updates from the store-level databases, and they accessed entries in the central Persons of Interest database created by other stores within the same regional vicinity.

AxxonSoft

The one store using AxxonSoft reported that the system had two server connections: a single server connected to an isolated network linked up with the FRT cameras, and a second network connection that allowed external access for support from SEQ, who installed the system. The system was also accessible from three in-store workstations: one in the Loss Prevention Office, and two at the Returns Desk to support a verification system.

SEQ reported that only their personnel could register the in-store workstations with the server and install the client software that enabled access to the FRT application. SEQ accessed and managed the server remotely. The company reported that AxxonSoft did not have access to the FRT server.

AxxonSoft captured a five-to-seven second-long video clip of each person who entered the store. The recorded clips were then stored in a Visitor database for 30 to 60 days, depending on the volume of daily recordings. AxxonSoft's software analyzed the video feed and calculated facial biometrics for comparison to its version of a Persons of Interest database. According to SEQ and the store manager, new biometrics without matches were stored in a Visitor database for three hours.

The store manager described the process for building AxxonSoft's Persons of Interest database as follows. With their cell phone, the security manager would take a photo of an individual allegedly involved in an incident. Security personnel then entered the individual's information into the database. This entry included a facial image taken from the cell phone photo along with additional descriptors. For AxxonSoft, these additional descriptors were non-restricted, open-entry text fields that may include name and date of birth, identifiers such as tattoos or scars, details about the incident, and, if relevant, a police file number. The photo would be used to generate a facial biometric, which was added to the database entry. All of this information was stored indefinitely in the Persons of Interest database, or until manually deleted.

According to SEQ and the store, the AxxonSoft system did not connect to any type of central server, so the Persons of Interest database was not shared with other stores. However, SEQ noted that the system did contain an export feature for images (but not facial biometrics). Users could copy or transport copies of images to external parties.

This store also used AxxonSoft as a Returns Desk Verification System, to confirm that individuals presenting themselves at the returns desk had entered the store with the products they wanted to return. Personnel at the returns desk would manually activate the verification system when a person approached the returns desk. The system then captured a static image from a live video feed, generated facial biometrics, and ran a comparison against the Visitor database with facial biometrics of anyone who had entered the store during the previous three hours. Staff then reviewed a recorded video clip of the person entering the store to verify whether the individual had the item for return with them upon arrival. If the individual did not appear to have the item when entering, staff would alert management or security.

5 FINDINGS

5.1 Were the stores required to obtain consent, and did they?

5.1.1 Was consent required for collection?

In most cases, PIPA requires organizations to obtain consent, either explicitly or implicitly, before collecting, using, or disclosing personal information.[12] PIPA specifies certain exceptions to this requirement that allow for the collection of personal information without consent.[13] No such exceptions applied in this case. Therefore, it was incumbent on the stores to show that individuals gave consent for the collection of their personal information.

Finding 1: The stores were required to obtain consent prior to, or at the time of, collecting individuals' images and creating facial biometrics.

5.1.2 Was notification sufficient for consent?

Advance notification of what information an organization intends to collect is a legally required element of consent. Section 7(1) of PIPA states that individuals have not given consent unless the organization provides them with the form of notice described in s. 10(1), which requires that organizations must disclose the purposes for collection of personal information before or at the time of collection.

In this case, the FRT systems collected or created two distinct forms of personal information as visitors entered the stores: collected images or videos of their faces and, subsequently, generated facial biometrics rendered from those images.

The subsequent biometric collection of personal information, in particular, would not be evident to a customer. For that reason, it would need to be clearly and specifically drawn to a

[12] Section 6.
[13] Sections 6, 12 and 15.

person's attention. That notice would be in addition to any forewarning regarding data collection by the FRT cameras.

In short, the stores were required to notify and obtain consent from individuals for each type of collection of personal information by FRT.[14] This notice is in addition to any notice about collection of personal information by the stores' separate surveillance system.

Proper notice must include setting out, in detail, the purposes for collection in an understandable way that affords a person the opportunity to give meaningful and informed consent.[15] Overly broad statements about purposes for collecting information are insufficient; they do not allow individuals to make informed decisions.[16] Because biometrics are more sensitive and complex than images captured by traditional video surveillance, FRT necessitates a more detailed explanation of collection purposes than traditional solutions require.[17]

The four stores posted notices at their entrance doors, with each referring to the use of FRT or biometrics. However, the wording within each notice differed. Each notice is assessed below, as to whether it met notice requirements of s. 10(1).

Store 1

This notice stated, in part: "these premises are monitored by video surveillance that may include the use of electronic and/or biometric surveillance technologies."

This notice did not state the purposes for the collection of personal information. A further shortcoming: stating that biometric surveillance *"*may*"* be in use did not reflect that the store continuously employed such technology. Additionally, the average person cannot reasonably be expected to understand how their information may be handled by "biometric surveillance technologies," let alone the implications and risks of this new technology. Consent requires that an individual understands what they are agreeing to – and the posted notification clearly failed to adequately alert the public in this case.

This store failed to meet notification requirements under PIPA.

Store 2

This notice stated, in part: "facial recognition technology is being used on these premises to protect our customers and our business."

---

[14] Section 10(1). See also OIPC Report P16-01. 2016 BCIPC 56 at p. 16. https://www.oipc.bc.ca/audit-reports/2111.
[15] Order P11-02, 2011 BCIPC 16 at para. 104, https://www.oipc.bc.ca/orders/1422; Order P21-06, 2021 BCIPC 35 at para. 101, https://www.oipc.bc.ca/orders/3560; and Office of the Privacy Commissioner of Canada and Offices of the Information and Privacy Commissioner of Alberta and BC, 2018. Obtaining meaningful consent, see p. 3, para. 2. https://www.oipc.bc.ca/guidance-documents/2255.
[16] Order P11-02, 2011 BCIPC 16 at para. 106. https://www.oipc.bc.ca/orders/1422.
[17] Joint Investigation of Cadillac Fairview Corporation: https://www.oipc.bc.ca/investigation-reports/3480.

The purpose, as set out, is so broad that the statement would relay no specific meaning to the average person. Furthermore, the notice does not explain what FRT entails or the nature of the personal information collected. One cannot reasonably assume that members of the public understand what FRT is, nor its privacy implications.

This store failed to meet notification requirements under PIPA.

Stores 3 and 4

The remaining two stores' notices stated: "video surveillance cameras and FRT (also known as biometrics) are used on these premises for the protection of our customers and staff. These technologies are also used to support asset protection, loss prevention and to prevent persons of interest from conducting further crime. The images are for internal use only, except as required by law or as part of a legal investigation."

This notice does not spell out what "FRT" is. That is an important oversight because the abbreviation is not yet well-known or widely understood. Using the full phrase "facial recognition technology" along with a basic explanation of its workings would have provided a more accurate description of the stores' data-collection activities. Even so, North American society is not yet at the point where it is reasonable to assume that the majority of the population understands what personal information FRT collects, or creates, as well as the technology's privacy implications.

Despite these stores' more robust notifications, they failed to meet notification requirements under PIPA.

Taken together, these notices lack sufficient detail. Said another way, as in OIPC Order P21-06, "the purposes should be stated as precisely as possible so that the needs of the organization to collect and use the information can be carefully assessed against the privacy rights of the individual."[18]

In this case, the stores used FRT in addition to video surveillance. The stores posted notifications stating that their premises were "monitored by video surveillance" or that "video surveillance cameras are used." These terms and the technology accompanying them have been a part of North American society for decades, in both private and public settings.[19] As such, it is reasonable to assume that our population has generally developed an understanding of what personal information is being collected by video surveillance: namely images or likenesses. Understanding what is being collected, and how, allows individuals to make informed decisions about what they consent to, should they choose to enter an establishment that notifies them that the premises are monitored by video surveillance and details how their information will be used.

[18] Order P21-06. 2021 BCIPC 35 at para. 53. https://www.oipc.bc.ca/orders/3560.
[19] Investigation P98-012. Video surveillance by public bodies: a discussion. https://www.oipc.bc.ca/investigation-reports/1259.

By comparison, the terms "biometric surveillance," "biometrics," "facial recognition technology," and "FRT" are not yet commonly understood or familiar. Without a common understanding, using the above terms is both vague and overly broad, leaving room for interpretations that may lead to inaccurate understandings of precisely what is collected and how personal information might be used.

The term "biometrics" encompasses a wide variety of biological measurements. FRT is only one form and one type. As the Privacy Commissioner of Canada observed, the word "biometrics" originally meant the mathematical measuring of biological characteristics, but:

> Nowadays, the term refers to a range of techniques, devices and systems that enable machines to recognize individuals, or confirm or authenticate their identities. Such systems measure and analyze people's physical and behavioural attributes, such as facial features, voice patterns, fingerprints, palm prints, finger and palm vein patterns, structures of the eye (iris or retina), or gait.[20]

Even if some or many individuals understand what is meant by "biometrics" or "FRT," the stores did not provide additional information detailing what personal information was being collected, nor did they provide sufficient detail about the intended purposes. If a notice does not convey meaningful details that inform people about the precise nature of collection processes and purposes, an organization will fail to meet its notification requirements under PIPA. That failure applies to notices posted at each of the stores involved in this investigation.

All four stores should have provided fulsome notifications to better inform individuals about FRT collecting their images and creating facial biometrics. As well, the stores should have detailed their precise purposes for employing FRT. The most serious failure of the notices is that they assume everyone will understand what FRT or facial biometrics are, as well as the implications and risks of disclosing highly sensitive and unique personal identifiers.

Finding 2: The stores did not meet the notification requirements of s. 10 of PIPA.

5.1.3 Did the stores obtain consent?

Under PIPA, consent is not legally valid where notification is insufficient under s.10(1). In this case, the stores failed to provide adequate notification. Nonetheless, the OIPC decided to evaluate the matter of consent in this investigation for the sake of completeness of analysis.

When assessing consent requirements, organizations must consider whether to rely on *implicit* or *explicit* consent.

Implicit consent is given when the purposes behind the collection are obvious, before or at the time of collection; individuals then voluntarily provide their personal information to the

[20] https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/gd_bio_201102/.

organization for the stated purpose.[21] If the means and purpose of collection is not obvious, then implicit consent is not possible.

The OIPC defines explicit consent, also known as express consent, as follows:

> [A]n individual, knowing what personal information is being collected and for what purposes, willingly agrees to [their] personal information being collected, used and disclosed as notified. Express consent can be given in writing or verbally. If you rely on verbal consent, remember that you may have to prove later that the consent was actually given by the individual.[22]

All four stores stated that they obtained implicit consent to collect personal information from individuals entering their locations. However, the purposes for collecting facial biometrics would not have been obvious to an average customer, including the creation of the persons of interest database. The stores are therefore unable to rely on implicit consent. Where information is highly sensitive, such as facial biometrics, only explicit consent would be valid.

Explicit consent must be obtained when:

- the information being collected is sensitive in nature;
- the collection, use, or disclosure falls outside the individual's reasonable expectation; or
- the collection, use, or disclosure creates a meaningful, residual risk of significant harm.[23]

Facial biometrics are especially sensitive, distinctive, and immutable pieces of personal information.[24] Their collection, use, and disclosure certainly go beyond people's reasonable expectation when they enter retail stores, and FRT creates a substantial and lasting risk of significant harm. The uniqueness and longevity of this biometric data can make this information attractive for misuse, as it becomes another potential tool or target that can be used to compromise an individual's identity. In the wrong hands, this data can be used for identity theft and financial or other significant harms. For all of these reasons, the four Canadian Tire stores were required to obtain explicit consent to collect facial biometrics. They did not attempt to do so, verbally or in writing.

---

[21] See s. 8 of PIPA and OIPC Audit Report P16-01. 2016 BCIPC 56 p.18. Over-collected and Overexposed: Surveillance and Privacy Compliance in a Medical Clinic.

[22] OIPC. October 2015. A Guide to B.C.'s Personal Information Protection Act for Businesses and Organizations. p. 14. https://www.oipc.bc.ca/guidance-documents/1438.

[23] Office of the Privacy Commissioner of Canada and Offices of the Information and Privacy Commissioner of Alberta and BC, 2018. Obtaining Meaningful Consent. Explicit consent is also referred to as express consent in the guidelines. See also Royal Bank of Canada v Trang, 2016 SCC 50 paras 23 & 34 2016 SCC 50 (CanLII) | Royal Bank of Canada v. Trang | CanLII; and Office of the Privacy Commissioner of Canada's PIPEDA's report on the Investigation into Home Depot of Canada Inc.'s compliance with PIPEDA (PIPEDA Findings #2023-001: Investigation into Home Depot of Canada Inc.'s compliance with PIPEDA - Office of the Privacy Commissioner of Canada).

[24] Order P21-08 (Clearview AI). 2021. BCIPC 73 at para. 41. https://www.oipc.bc.ca/orders/3610.

Obtaining explicit consent in a retail environment would undoubtedly be a significant undertaking. But such an undertaking is both necessary, proportionate, and commensurate with asking people to hand over to a retailer extraordinarily detailed and sensitive personal information.

Finding 3: The stores did not obtain implicit or explicit consent for the collection, use, or disclosure of biometric information via FRT, contrary to ss. 7 and 8 of PIPA.

5.2 Did the stores collect and use personal information for appropriate purposes?

Even if the stores obtained consent, which they failed to do, they would still be legally required to demonstrate that the collection and use of personal information was only for purposes that a reasonable person would consider appropriate in the circumstances.[25]

When evaluating the reasonable person standard, previous OIPC Orders[26] have considered the following factors, which are relevant in this case:

- the amount of personal information collected;
- the sensitivity of the personal information;
- the likelihood of effectiveness in achieving a stated purpose; and
- whether less intrusive alternatives were available.[27]

5.2.1 Amount of personal information collected

The amount of personal information collected (from customers, staff, contractors, and other visitors) was voluminous. The stores reported that hundreds of individuals of all ages, including minors, entered their stores each day. Over the course of a month, the images of thousands of people going about their shopping, and not involved in malicious behaviour, were captured by the FRT systems. The vast amount of information collected is one indicator of unreasonableness.

[25] Order P11-02. 2011 BCIPC 16. And P21-06. 2021 BCIPC 35. https://www.oipc.bc.ca/orders/1422.
[26] Order P05-01. 2005 BCIPCD 4., Orders P12-01. 2012 BCIPC 25., P13-02. 2013 BCIPC No. 24., and P21-06. 2021 BCIPC 35.
[27] This list is not exhaustive, as other factors may apply depending on the particular circumstances. The relevant factors may vary from case to case.

5.2.2 Sensitivity of the personal information

Facial biometrics are an especially personal kind of identifier. The Commissioners of Canada, Québec, Alberta and British Columbia stated in their joint investigation of Clearview AI in 2021:

> Biometric information is distinctive, unlikely to vary over time, difficult to change and largely unique to the individual. Facial biometric data is particularly sensitive given that it is a key to an individual's identity, supporting the ability to identify and surveil individuals.[28]

Similar observations were made by the OIPC more than a decade ago:

> 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. [29]

In Canada, as in most western democracies, the collection of biometric information has come under intense legal scrutiny. Legislation significantly restricting or limiting relevant data processing has been passed or is proposed in Québec, several US states, and the European Union.[30] While each jurisdiction approaches this issue differently, common ground has been established. Data-protection authorities largely agree that FRT deals with sensitive information in an invasive manner.

Scrutiny over FRT's use has extended to law enforcement. Canada's privacy commissioners have called for a legal framework to limit use of this technology by police, due to the sensitivity of biometrics as well as concerns for privacy and human rights.[31]

In short, the type of personal information at issue in this case reaches the highest level of sensitivity.

5.2.3 The likelihood of effectiveness in achieving its stated purpose

Stores stated that the purposes for installing FRT and collecting and comparing images and facial biometrics of visitors, along with other personal information, were to:

- protect the safety of staff and customers;
- support asset protection and loss prevention; and

---

[28] Joint investigation of Clearview AI. https://www.oipc.bc.ca/investigation-reports/3505.
[29] Investigation Report F12-01 BCIPC 5. Para. 43. https://www.oipc.bc.ca/investigation-reports/1245.
[30] See: https://www.biometricupdate.com/202205/update-to-quebec-data-privacy-law-specifies-biometrics-use-notifications, https://www.americanbar.org/groups/business_law/publications/blt/2022/05/facial-recognition/, https://www.europarl.europa.eu/RegData/etudes/IDAN/2021/698021/EPRS_IDA(2021)698021_EN.pdf, https://gdpr-info.eu/art-9-gdpr/.
[31] https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/nr-c_220502/.

- prevent Persons of Interest from causing further dangerous situations or committing repeat offences.

It is essential that organizations establish a robust way to measure the effectiveness of any new technology that collects additional personal information *before* moving forward with putting that technology in place. This is usually done by comparing relevant metrics before and after implementation.

In this case, the stores did not provide any evidence of a systematic measurement system, and instead only provided anecdotal evidence of the frequency of theft and safety incidents before and after installation. Without a meaningful way to measure a technology's effectiveness, there is no real way to analyze this factor. Organizations—especially when considering collection of highly sensitive personal information—should have a clear idea of how to measure their stated purposes in order to assess continued effectiveness and demonstrate compliance.

Another related issue, at least as FRT technology currently operates, is the accuracy of the technology itself, which has been widely reported to falsely match facial biometrics of people of colour and women.[32] Store managers acknowledged they were aware that alerts could be inaccurate and had, therefore, routinely deployed staff to determine whether a match was legitimate by comparing database images to a visual observation of the individual. Again, without an accurate measurement system, it becomes difficult to assess how (and if) more theft and safety incidents were prevented, but this manual check by staff indicates the systems may not be effective. In some cases, a false identification has harmful consequences when otherwise innocent shoppers are followed or confronted based on an inaccurate match who would not otherwise be subject to such scrutiny.

Besides the system's accuracy, its effectiveness can also be judged against existing methods used by the stores to identify potential suspects. While evidence from store managers is that FRT helped in some cases to identify these individuals as soon as they arrived, the managers also stated that their security guards and managers usually knew the "bad actors" and could often recognise them without receiving FRT alerts. As the managers told investigators, the persons of interest were often professional thieves who would repeatedly return to a targeted location.

[32] See CBC News, Manitoba. October 19, 2022. First Nations man wants apology after being flagged as shoplifter, asked to leave Canadian Tire store. https://www.cbc.ca/news/canada/manitoba/first-nation-apology-store-accused-1.6620457. See discussion on the accuracy of FRT in the Report of findings: Joint investigation of Clearview AI, Inc. 2021. Paras. 91-97. https://www.oipc.bc.ca/investigation-reports/3505. See too the following: "NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software," National Institute of Standards and Technology (NIST), December 2019; "Black and Asian faces misidentified more often by facial recognition software," CBC News, December 2019, and "Federal study confirms racial bias of many facial-recognition systems, casts doubt on their expanding use," Washington Post, December 2019. Facial-recognition systems misidentified people of color more often than white people, according to a federal study - The Washington Post.

The investigation also found little evidence of FRT's effectiveness in enhancing customer and employee safety. Whether a person of interest was identified by FRT or by the visual recognition of an employee, the stores' next steps were the same. These involved deciding whether to observe the suspected person of interest or interact with them directly: including, in some cases, escorting them from the premises. In either case, and despite the potential seriousness of some incidents, store managers rarely reported contacting police for assistance.

5.2.4 Whether less intrusive alternatives had been attempted

Interviews with store managers revealed that they deployed less-intrusive means of protecting staff and customers, of protecting assets, and preventing loss, with a certain degree of success. For example, each of the stores is equipped with dozens of video surveillance cameras and employs security contractors or internal staff trained in theft prevention.

Store managers reported that, on occasions when they called police to assist during incidents of violence, theft, or vandalism, officers requested extracts of video surveillance to help identify individuals, rather than images or matches from the FRT system.

Store managers also said that FRT was rarely needed to identify a person of interest who returned to their stores. Those individuals were known and identifiable without FRT alerts. Indeed, the stores employ dedicated loss-prevention staff who remain on the lookout for persons of interest and any others who may attempt to shoplift, vandalize, or otherwise cause problems.

Arguably, the stores gained little by employing FRT on top of less-intrusive alternatives already in place. At most, FRT might alert store staff to a known suspect a little more quickly than might otherwise be the case.

While using technological solutions such as FRT may have some advantages in retail settings, the benefits must be weighed against the intrusiveness of collecting vast quantities of sensitive information. In this case, the marginal security advantage is not proportionate to the substantial risk of data breaches, identity theft, and other abuses.

Each store manager said that they purchased their FRT system after a vendor presentation and without first conducting a feasibility assessment or a privacy impact assessment, or otherwise considering the privacy rights of individual citizens. Organizations should assess and document the likely effectiveness of a particular solution, along with any impacts on privacy, before implementing new technologies that collect or use personal information.

The particulars of this case did not warrant collecting the facial biometrics of every individual (including minors) entering Canadian Tire stores in British Columbia. Factors contributing to that conclusion include: the amount and sensitivity of the information collected, issues of accuracy and limits to effectiveness with these FRT systems, and the availability of less intrusive

means to achieve stated purposes for data collection. In this case, a reasonable person would not consider the means appropriate to the ends.

Finding 4: The stores did not demonstrate a reasonable purpose, as required by ss. 11 and 14 of PIPA, to collect or use personal information through FRT.

5.3 Did the stores securely destroy personal information?

Even though the stores discontinued their use of FRT shortly after the investigation began, a question of what happened to the personal information that was collected remained. As the stores did not obtain consent for the collection of personal information through the FRT systems, and there was no reasonable purpose for them to have collected it in the first place, the stores were required to destroy all personal information collected to support their FRT system.

These personal information holdings[33] included:

- images or videos captured through the FRT system of each visitor entering the stores;
- images or videos of the individuals captured through cell phones and uploaded to the AxxonSoft system's Persons of Interest database;
- facial biometrics created from captured images of faces;
- in store Persons of Interest and Visitor databases;
- the central Persons of Interest database in the FaceFirst system held by SilverPoint (shared with other Canadian Tire stores);
- images or other personal information contained in alerts sent to managers or staff; and
- any other personal information, such as physical descriptors, collected with the intent of adding such information into the FRT system or related databases.

FRT systems and databases destroyed

In the case of the three stores using FaceFirst, the systems were decommissioned by store management, and SilverPoint reported wiping the server drives using a three-times overwriting process. Once this process was complete, the staff person who performed the erasure filled out data destruction forms and sent these to the stores.

SEQ, the third-party vendor who installed the AxxonSoft system at one store, confirmed that the data on the disk was removed using a Windows delete command during the decommissioning process. Using a basic delete function to decommission a server would have left data on the server drives that could be recovered (because the disks were not encrypted). As such, the OIPC directed the store to erase disks with a three-pass overwrite or to physically

[33] Unless otherwise specified, the personal information holding relates to both the FaceFirst and AxxonSoft FRT systems.

destroy non-operational disks. In response, the store had the server drives physically destroyed and provided a certificate of destruction to the OIPC.

The OIPC is satisfied that the FRT systems and their related databases within the custody of the stores have been securely destroyed.

6 RECOMMENDATIONS

6.1 Privacy management programs

The absence of consideration for people's right to privacy emboldened the stores to install security solutions that collected vast quantities of sensitive personal information in a manner that contravened the law. Namely, stores collected personal information without proper notice or consent, and the collection itself was not reasonable or proportionate when measured against intended purposes. The stores' non-authorized collection and use of facial biometrics put countless people at risk of harm.

This report documents what can go wrong when organizations lack effective, accountable privacy management programs. Privacy management programs aid organizations in meeting their legal obligations by setting out roles and responsibilities.[34] In this investigation, the Canadian Tire stores should have:

- documented organizational expectations and limits for the collection, use, and disclosure of personal information in fulsome privacy policies;
- conducted risk and feasibility assessments in advance of implementing new systems that collect or contain personal information;
- ensured contracted services align with organizational privacy policies; and
- monitored compliance with the law and organizational expectations.

Implementing accountable privacy management programs would have provided frameworks against which the stores could have critically analyzed whether to acquire the FaceFirst and AxxonSoft FRT systems as a security measure in the first place. In addition, even though the stores have removed their FRT systems, having a robust privacy management program would enable them to be better equipped to evaluate and protect other personal information they collect.

[34] See Getting accountability right with a privacy management program. https://www.oipc.bc.ca/guidance-documents/1435.

RECOMMENDATION 1

The stores should build and maintain robust privacy management programs that guide internal practices and contracted services.

6.2 Regulation of biometric security services and products

While organizations have responsibility under privacy legislation, governments enshrine societal expectations by defining what is permissible under the law through regulation and legislation.

The BC Government's Security Programs Division regulates and licenses security businesses whose primary function is the provision of security services and technologies. There is need for such regulation because allowing security professionals access to homes and businesses is a position of trust that requires accountable protection of these spaces from unauthorized access, theft, damage, or other harms. Protecting safety often entails collecting personal information, which must be protected.

In BC, the *Security Services Act* and Security Services Regulation apply to companies such as locksmiths, security guards, and those that install CCTV and alarm systems.[35] However, companies that provide highly intrusive biometric security services and products – like FRT – are not subject to the same level of oversight or licensing. This discrepancy represents a profound gap in regulation.

This investigation demonstrates the need for government to fix the regulatory gap. FRT and other biometric solutions are now sold and used in BC without parameters, controls, or accountability. These technologies are far more intrusive than other security solutions that government currently regulates. Companies and individuals who provide FRT and other biometric solutions should be subject to oversight, just as government controls CCTV and alarm companies. Government needs to promptly establish regulatory oversight to protect British Columbians.

[35] See Security Services Regulation, BC Reg 207/2008, s. 15.

RECOMMENDATION 2

BC Government should amend the *Security Services Act* or similar enactment to explicitly regulate the sale or installation of technologies that capture biometric information.

6.3 Enhancements to PIPA

The existing legislative framework under PIPA, which is largely complaint-driven, does not adequately address special issues around the collection, use, and disclosure of sensitive biometric information created and used by facial recognition and similar technologies. In the criminal context, legislation governs the collection and use of biometric information in the form of mugshots,[36] DNA,[37] and fingerprints.[38] To protect the privacy of British Columbians, PIPA should be amended to impose specific obligations including, at minimum, that organizations notify the OIPC – whether by submission of a Privacy Impact Assessment or otherwise – that they intend to provide or implement any technology product or service that involves the collection, use, or disclosure of biometric information.

Examples of such a positive obligation exist both internationally and in Canada. The recommendation would harmonize PIPA with other jurisdictions. Many US states have passed biometrics laws, most notably Illinois.[39] Across the Atlantic, the draft EU *Artificial Intelligence Act*[40] outlaws some uses of artificial intelligence that involve biometric collection. This Act specifically limits the use of real-time FRT by law enforcement to only the most serious and exceptional circumstances.

Closer to home, Québec's recently amended private sector privacy law[41] includes provisions that require organizations to disclose any biometric database to the Commission d'accès à l'information (CAI). This requirement to notify the regulator of the use of biometrics allows the public and the regulator a greater awareness and oversight of how these technologies are being employed.

---

[36] See *Identification of Criminals Act*, RSC 1985, c I-1.
[37] See *Criminal Code*, RSC 1985, c C-46, ss 487.05-487.092; *DNA Identification Act*, SC 1998, c. 37.
[38] See *Identification of Criminals Act*, *supra* note 2, s 2; *Criminal Code*, *supra* note 3, s. 487.06(3).
[39] See *Biometric Information Privacy Act*, 740 ILCS 14 (2008). https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.
[40] See Proposal for a Regulation laying down harmonised rules on artificial intelligence" https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-european-approach-artificial-intelligence.
[41] See Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, 1st Sess, 42nd Leg, Québec, 2021 (assented to 22 September 2021), SQ 2021, c 25, amending *Act Respecting the Protection of Personal Information in the Private Sector*, CQLR c P-39.1. https://www.legisquebec.gouv.qc.ca/en/document/cs/p-39.1.

RECOMMENDATION 3

BC Government should amend PIPA to create additional obligations for organizations that collect, use, or disclose biometric information, including requiring notification to the OIPC.

7 SUMMARY OF FINDINGS AND RECOMMENDATIONS

This investigation makes four findings of non-compliance with PIPA summarized as follows:

- The stores were required to obtain consent prior to, or at the time of, collecting individuals' images and creating facial biometrics.
- The stores did not meet the notification requirements of s. 10 of PIPA.
- The stores did not obtain implicit, or explicit, consent for the collection or use of biometric information via FRT, contrary to ss. 7 and 8 of PIPA.
- The stores did not demonstrate a reasonable purpose, as required by ss. 11 and 14 of PIPA, to collect or use personal information through FRT.

Store managers have addressed most of these non-compliance concerns by removing the FRT systems from their retail locations and destroying personal information stored in system databases. To help equip the stores to make better decisions in the future and to aid in managing the other personal information they currently maintain, this report makes one recommendation to the individual stores operating in BC:

1. The stores should build and maintain robust privacy management programs that guide internal practices and contracted services.

This report also makes two recommendations for the BC government:

2. BC Government should amend the *Security Services Act* or similar enactments to explicitly regulate the sale or installation of technologies that capture biometric information.

3. BC Government should amend PIPA to create additional obligations for organizations that collect, use, or disclose biometric information, including requiring notification to the OIPC.

8 CONCLUSION

Facial recognition technology is a powerful tool that requires considered control and oversight. It is understandable that organizations will reach for new technologies that promise easy solutions to age-old challenges. However, as with most things, it is never quite that straightforward or simple.

Many factors must be considered before deploying a new technology. The *Personal Information Protection Act* requires it. How much personal information is being collected? How sensitive is that personal information? Once collected, does the technology even achieve its promised outcomes? Are there less intrusive methods of achieving the same ends? These considerations and others must be weighed to determine whether the deployment of a particular technology is a proportionate response to the challenges at hand.

When taken together, FRT represents a particular technology that is highly invasive. It is for that reason that legislators and policy makers in democracies around the globe have banned, or significantly restricted, uses of FRT, among other biometric technologies. FRT should only be used when it is determined to be a proportionate response to an organizational challenge.

It is in this context that retailers need to tread very carefully when considering the use of this kind of technology.

Our Provincial Government must also ensure the public interest is met by developing regulatory tools that are fit for purpose

Innovative technologies can and will continue to play an important role in our lives. However, those advancements can only be made with the trust of the citizenry. A fundamental aspect of that trust is respect for the privacy rights of citizens.

9 ACKNOWLEDGEMENTS

I thank the store management and other staff who contributed to this review by providing forthright documentation and making themselves, and key staff, available for interviews.

I would also like to thank Investigator Nanci Bond, IT security consultant Ken Prosser, and Director of Audit and System Review, Tanya Allen, for conducting this investigation and drafting this report.

ORIGINAL SIGNED BY

Michael McEvoy, Information and Privacy Commissioner for BC
April 20, 2023