January 5, 2023

#AI Facial Recognition Technology in the Retail Industry

By: Gideon Christian

Issue Commented On: OIPC Investigation Report 23-02: Canadian Tire Associate Dealers' use of facial recognition technology, 2023 BCIPC 17

One summer day in 2023, I entered a Walmart store in Calgary, Alberta, and purchased three standing fans. Upon assembling the fans at home, I discovered that one was malfunctioning. I immediately decided to return it to the store. Armed with my purchase receipt, I walked to the return desk. After a brief wait in line, I presented the defective fan and the receipt to the Walmart staff. To my astonishment, he informed me that the receipt was not necessary and casually remarked, “You bought three of these today, right?” Concealing my surprise, I affirmed. He swiftly processed my refund.

As I left the store, I wondered: “How did he know I bought three fans?” I began to suspect the store’s use of facial recognition technology, believing it to be the only reasonable explanation for his knowledge. But that was only my suspicion, and as the legal saying goes, "suspicion, however strong, is not evidence." This incident lingered in my mind for months, leading me to finally send an email to Walmart Corporation asking about their use of facial recognition technology in Alberta stores and my rights regarding the collection and processing of my biometric information. The response from Walmart was swift: they confirmed that Walmart Canada does not use facial recognition in any of their stores in Canada.

Facial Recognition Technology (FRT) is an artificial intelligence-based biometric system that employs computer vision to identify individuals by their unique facial features. In the retail industry, this involves installing high-quality surveillance cameras in stores. These cameras capture video footage of customers, from which still images of their faces are extracted. The FRT system utilizes these images to generate a unique set of mathematical and biometric information tied to the individual's activities in the store.

One application of FRT in the retail sector is in the return process of purchased items. FRT could be used to pull up information about customers who try to return items to the stores for refund, to ensure that they are not returning stolen items for a cash refund. Additionally, FRT plays a role in identifying "persons of interest" — individuals who have previously been caught, suspected, or accused of shoplifting. Their biometric information is stored in the store’s database. When these individuals enter any store associated with the retail chain, staff are automatically alerted. This can result in the individuals being either removed from the premises or closely monitored by store security. While FRT can be a useful tool for the retail industry in fraud prevention, its use raises significant concerns relating to privacy, gender, and racial bias.

“Shopping While Black” Goes Digital

The retail industry has actively embraced various human and technological resources to combat the rise in shoplifting, also known as fraud prevention. This arsenal includes security guards, human receipt checks (a familiar sight in Costco stores), auto-lock wheels on shopping carts, RFID tags triggering alarms at store exits, and CCTV cameras. A recent addition to this array is FRT, arguably the most controversial tool in the fraud prevention toolkit.

There are many issues surrounding the use of FRT in the retail industry. Among these are its highly invasive nature and its well-documented error rate disparities across racial and gender lines. Studies have shown that while FRT boasts over a 99% accuracy rate in recognizing White male faces, its performance significantly deteriorates when identifying people of colour, particularly Black women, exhibiting a much higher error rate. This discrepancy means that these demographic groups are at an increased risk of being mistakenly flagged as "persons of interest" in stores, leading to undue surveillance or even false criminal accusations.

A recent investigation by the US Federal Trade Commission (FTC) revealed that the deployment of FRT by Rite Aid, a major US retail pharmacy, “in stores located in plurality-Black and Asian communities” was done without any effort to consider and mitigate the risks of racial bias. Hence, for Black people and people of colour, this takes the concept of “shopping while Black” to a whole new digital realm, the realm of smart technology, or what I shall refer to as the ‘smartosphere’.

However, concerns about FRT's invasiveness are not limited to specific racial and gender groups; its intrusive nature is a universal issue. The use of this technology in the retail industry, in its current form, poses a threat to the privacy of all individuals, regardless of race or gender.

Photo comment: Studies have shown that FRT has a high error rate recognizing the faces of people of colour.

Justification for the Use of FRT in the Retail Industry

If FRT is recognized as invasive and intrusive, how then does the retail industry justify its use on customers? The primary rationale often cited by the industry is the significant impact of their perennial adversary – organized retail crime, particularly shoplifting. The industry has reported substantial financial losses attributed to this criminal activity, backing their claims with data to illustrate the severity of the issue.

For instance, in 2023, the US-based National Retail Foundation reported annual losses of approximately $45 billion to organized retail crime. This staggering figure might appear to rationalize the use of FRT as a means to mitigate losses. However, as Los Angeles Times columnist Michael Hiltzik later revealed, the $45 billion figure was a huge exaggeration that was fabricated by the industry. That notwithstanding, the inflated figure circulated rapidly, at the speed of fake news, and was leveraged to justify more aggressive, and sometimes abusive, approaches to shoplifting. An ex-US president even suggested that shoplifters be shot when leaving the store.

To this day, fraud prevention remains a key argument for the retail industry's deployment of FRT in their stores. This brings us to a critical question: Do the criminal actions of a few outlaws justify the imposition of such invasive and intrusive technology on the general population of customers – the majority of whom are honest, law-abiding individuals patronizing these businesses for legitimate purposes? To further delve into this issue, let us examine an investigation into the use of FRT by some outlets of a major Canadian retail chain – the Canadian Tire Corporation.

Investigation into Canadian Tire Corporation's Use of FRT

The Canadian Tire Corporation is a Canadian retail outlet that operates chains of automotive, hardware, and houseware stores in major Canadian cities. Some of the stores are run by independent associate dealers. Sometime in 2018, some of the Canadian Tire stores in British Columbia initiated the deployment of FRT for fraud prevention. High-definition cameras were installed at store entrances, exits, checkout counters, and return desks. These cameras captured images of all individuals entering the stores, which were then stored in a database. Additionally, the stores maintained a separate database for "Persons of Interest" – individuals previously involved in incidents like shoplifting in the stores. This database also included manually captured and uploaded images of suspected shoplifters, which were then converted into biometric information by the FRT.

The high-definition cameras captured the facial images of all persons entering the stores. These images were then used by the FRT to create unique biometric templates of individuals' faces. This biometric data was used to scan the "Persons of Interest" database for potential matches. If a match was found, the system automatically alerted store management and security personnel. The matched image and its corresponding biometric information were stored in the "Persons of Interest" database, ranging from two years to indefinitely, or until manually deleted. If there was no match, the information was retained for 30 to 60 days.

At the return desk, the FRT cameras were used to scan the faces of individuals returning items. The FRT system, which was manually activated by staff, captured a still image of the customer to generate facial biometrics, which was then used to pull up video recordings of the individual's store visit, verifying whether they possessed the item upon entry.

In 2021, the Office of the Information and Privacy Commissioner for British Columbia (OIPC) launched an investigation into the use of FRT by Canadian Tire stores in the province. This investigation aimed to determine if the use of the technology by the stores violated British Columbia's *Personal Information Protection Act*, SBC 2003, c 63 (*PIPA*). On becoming aware of the investigation, the affected stores promptly dismantled their FRT systems.

Sections 6 – 8 of *PIPA* mandates that organizations obtain consent from individuals when collecting, using, or disclosing their personal information. Accordingly, the OIPC's investigation primarily focused on determining whether Canadian Tire customers were informed about the use of FRT in the stores, and whether they consented to the collection and processing of their biometric information. Another critical aspect was evaluating the reasonableness and justification for collecting and using the highly sensitive biometric information.

While the OIPC's final Report acknowledged that the stores had displayed robust notices informing visitors of video surveillance, which might include biometric and facial recognition technologies, it found that these notices were insufficient for obtaining consent. The rationale was that "the average person cannot reasonably be expected to understand the handling of their information by 'biometric surveillance technologies,' nor comprehend the implications and risks of this emerging technology" (at 12). Furthermore, while visitors might implicitly consent to video surveillance upon entering the store, this consent does not automatically extend to the subsequent generation and use of biometric information via FRT.

The Report was also critical of the volume of personal data collected through FRT, including biometric information of individuals of all ages, even children (at 16). The OIPC observed that the sheer amount of data collected was neither reasonable nor effective in meeting the stated goal of fraud prevention. The Report highlighted that within a single month, "the images of thousands of people engaged in regular shopping activities, and not involved in any malicious behavior, were captured by the FRT systems" (at 16). This extensive data collection was deemed an indicator of unreasonableness.

Therefore, the investigation concluded that the extensive breach of the privacy rights of thousands of customers by the stores was not justified by their rationale of preventing retail fraud committed by a few malicious individuals in organized retail crime.

A crucial issue highlighted in the OIPC report, yet not thoroughly investigated, pertains to the accuracy rate of FRT among people of colour. The Report acknowledges the tendency for false identifications within this demographic, which can lead to serious repercussions. Innocent customers, particularly people of colour and Indigenous people, may face unjust treatment in stores, such as being unfairly followed, subjected to excessive scrutiny or surveillance, or even confronted based on erroneous identifications by the technology.

While the OIPC expressed approval of the store's decision to discontinue the use of FRT and the destruction of the collected biometric information, the scope of their investigation could have been more extensive. Acknowledging the problematic accuracy rate of FRT for people of colour, the OIPC should have delved deeper into the racial and gender composition of individuals in the "Person of Interest" database. An analysis of the representation of Indigenous people, people of colour, and women in the database would have provided a clearer understanding of the risks posed by the store's use of FRT to these specific demographic groups and measures, if any, taken by the stores to mitigate these risks.

Furthermore, given the unlawful collection and use of personal information in the "Persons of Interest" database, the OIPC should have mandated that the Canadian Tire stores notify the affected individuals. Such communication would inform them about the unlawful collection and use of their personal information and reassure them that their information has now been destroyed.

There have been news reports of Canadian Tires stores in other provinces in Canada using this technology. Regrettably, unlike in British Columbia, the information and privacy commissioners in these other provinces have not yet initiated investigations into the use of this technology. This lack of action is a cause for concern, especially considering the issues highlighted by the British Columbia investigation.

Conclusion

The OIPC investigation has shed light on both the risks and the unreasonableness of deploying FRT in the retail industry. The reality is that the number of individuals involved in the illegal act of shoplifting pales in comparison to the vast majority who frequent retail stores for legitimate purposes. Retail stores should not, and must not, infringe upon the privacy rights of the general customer base in an effort to apprehend or deter a relatively small number of shoplifters. As a society, we cannot afford to sacrifice the privacy rights of every customer (and vast numbers of customers collectively) entering a retail outlet in an attempt to prevent fraud by very few individuals. The retail industry should consider other, less invasive methods of addressing organized retail crime. Despite its power as a tool, FRT is excessively intrusive, and not the appropriate solution for combating the longstanding issue of organized retail fraud.

This blog post contributes to a broader research project examining the racial, gender, and privacy impacts of AI Facial Recognition Technology. This project is generously funded by the Office of the Privacy Commissioner of Canada, reflecting a commitment to understanding and addressing the multifaceted challenges posed by this emerging technology.

This post may be cited as: Gideon Christian, "#AI Facial Recognition Technology in the Retail Industry" (5 January 2024), online: ABlawg, http://ablawg.ca/wp-content/uploads/2024/01/Blog_GC_AI_Facial_Recognition.pdf

To subscribe to ABlawg by email or RSS feed, please go to http://ablawg.ca

Follow us on Twitter @ABlawg