Office of the Information and
Privacy Commissioner of Alberta

Commissariat
à la protection de la
vie privée du Canada

Office of the
Privacy Commissioner
of Canada

oipc
OFFICE OF THE
INFORMATION &
PRIVACY COMMISSIONER
FOR BRITISH COLUMBIA

Investigation Report P2020-IR-01

Joint investigation of The Cadillac Fairview Corporation Ltd. by the Information and Privacy Commissioner of Alberta, the Privacy Commissioner of Canada, and the Information and Privacy Commissioner for British Columbia

October 29, 2020

The Cadillac Fairview Corporation Ltd.

OIPC AB 009324; OPC PIPEDA-036698; OIPC BC P18-76168

Table of Contents

Overview

The Office of the Privacy Commissioner of Canada (OPC), Office of the Information and Privacy Commissioner of Alberta (OIPC AB) and the Office of the Information and Privacy Commissioner for British Columbia (OIPC BC), collectively referred to as “the Offices” commenced a joint investigation[1,2] to examine whether The Cadillac Fairview Corporation Limited (CFCL) was collecting and using personal information of visitors to its Canadian malls, without valid consent, via:

i. Anonymous Video Analytics (AVA) technology installed in “wayfinding” directories; and
ii. mobile device geolocation tracking technologies.

Our findings in respect of these two issues are detailed below.

CFCL collected and used personal information, including sensitive biometric information, via the AVA technology without valid consent.

The AVA technology: (i) took temporary digital images of the faces of any individual within the field of view of the camera in the directory (retained in computer memory briefly during processing); (ii) used facial recognition software to convert those images into biometric numerical representations of the individual faces (sensitive personal information that could be used to identify individuals based on their unique facial features); and (iii) used that information to assess age range and gender.

CFCL represented that the numerical representations were not retained beyond processing. However, our investigation revealed that CFCL’s AVA service provider had collected and stored approximately 5 million numerical representations of faces on CFCL’s behalf, on a decommissioned server, for no apparent purpose and with no justification.

CFCL explained that it collected information via AVA for purposes of monitoring foot traffic patterns and predicting demographic information about mall visitors. We found no evidence that CFCL had used the biometric information, including any of the retained numerical representations, for identification purposes.

CFCL also retained approximately 16 hours of video recordings, some including audio, which it had captured during a calibration (or testing) phase of the technology at two malls.

[1] Throughout this report the terms “we” and “our” are used frequently. When used outside of the context of a quoted document, these terms refer to the collective of the OPC, OIPC AB and OIPC BC.

[2] The three Offices subsequently entered into an information sharing arrangement with the Commission d’accès à l’information du Québec (“CAI”) in March 2019 as it had also initiated an investigation into CFCL’s use of AVA technology, though the CAI continued its investigation independently.

CFCL asserted that to the extent that it required consent, such consent was obtained via its privacy policy. We found that this was inadequate. Firstly, an individual would not, while using a mall directory, reasonably expect their image to be captured and used to create a biometric representation of their face, which is sensitive personal information, or for that biometric information to be used to guess their approximate age and gender. As such, CFCL should have obtained express opt-in consent. Further, we reviewed CFCL's privacy policy and determined that the language was overly broad, and buried in the middle of a 5,000 word document, which would not be easily accessible to individuals while they are engaging with a mall directory. We found that the privacy policy language was not sufficient to support meaningful consent for CFCL's AVA practices.

Finally, we noted that while shoppers were directed, by stickers displayed at mall entrances, to visit guest services to obtain a copy of CFCL's privacy policy, when we asked a guest services employee at one of CFCL's malls for that policy, they were confused by the request.

As a result of these findings, we made several recommendations. We recommended that CFCL either: (i) obtain meaningful express opt-in consent and allow individuals to use its mall directories without having to submit to the collection and use of their sensitive biometric information; or (ii) cease use of its AVA technology. While CFCL expressly disagreed with our findings, it advised that it had ceased use of the technology in July 2018, and that it had no current plans to resume that use. CFCL has also, pursuant to further recommendations by our Offices, deleted the numerical representations of faces and audio/video recordings in its possession which were not required for legal purposes. It has confirmed that what information has been retained will not be used for any other purposes outside of those required for compliance with the law. CFCL also provided privacy-related training to guest services employees. As a result, we found the matter to be **well-founded and resolved**.

Our Offices asked CFCL to provide a commitment to follow our recommendations with respect to ensuring valid consent if they were to resume use of AVA technology in the future. CFCL indicated that if it did resume use of the AVA technology, it would obtain adequate consent, "in accordance with the applicable privacy legislation and consistent with the *Guidelines for obtaining meaningful consent"*. However, it refused to commit to obtaining express opt-in consent consistent with our recommendations. We find this concerning given that CFCL disagreed with our analysis and interpretation of the law in this case. For example, CFCL continues to maintain, contrary to our findings, that they were not collecting personal information via the AVA technology.

CFCL did not collect the location information of identifiable individuals via mobile device tracking technology in its malls, such that it did not require consent for the practice.

We found that the information collected from mobile devices of shoppers, who were not logged into Wi-Fi in CFCL malls, did not constitute personal information. More specifically, the hashed and randomized MAC address (device identifier), coupled with non-granular "zone" geolocation information collected using Wi-Fi triangulation, did not constitute personal information in this context, as there was not a serious possibility that this information could be linked, either alone or with other available information, with the mobile device holder.

With respect to individuals who log in to CFCL's free Wi-Fi service, via a process that required them to provide personal information, we originally understood, based on the evidence gathered during our investigation, including from CFCL and its Wi-Fi service provider, that CFCL was collecting triangulated device geolocation information and linking it with identifiable device users' Wi-Fi accounts. We therefore made certain preliminary recommendations to CFCL with respect to the consent we would expect for this practice. However, in response to a preliminary report issued by our Offices, CFCL clarified, and its third-party Wi-Fi service provider verified, that the geolocation information described above could not in any practical manner be associated with, or linked to, logged-in Wi-Fi accounts, such that it was not personal information in that context. We therefore determined the matter to be **not well-founded**.

We did note, however, that CFCL was seeking consent for "special location-based offers", despite the fact that it was not engaged in the practice. Further to our recommendation, CFCL did remove such language from its privacy policy, and added language making clear what limited location information is collected and associated with Wi-Fi accounts (i.e., only the CFCL property in question).

Finally, we note that CFCL's third-party Wi-Fi service provider offers the option to associate triangulated "zone" information to accounts, and that CFCL did include, in its privacy policy, the prospect of using geolocation information to deliver location-based offers. We therefore recommended that CFCL commit to implementing our preliminary recommendations should it decide to activate this functionality and associate geolocation information with Wi-Fi accounts in future. Specifically, we would expect CFCL to: (i) support express consent for such geolocation practices via a clear and prominent notice on the Wi-Fi log-in page; and (ii) provide a clearly explained and easily accessible opt-out option. CFCL again refused, claiming that these recommendations were speculative.

Background

[1] This report of investigation examines The Cadillac Fairview Corporation Limited's ("CFCL") compliance with Canada's *Personal Information Protection and Electronic Documents Act* ("PIPEDA"), Alberta's' *Personal Information Protection Act* ("PIPA AB"), and British Columbia's *Personal Information Protection Act* ("PIPA BC") – referred to collectively as the "Acts".

[2] CFCL is one of the largest owners, operators and developers of offices, retail and mixed-use properties, including shopping malls, in North America.

[3] This joint investigation was launched in the wake of numerous media reports that raised questions and concerns about whether CFCL was collecting, using and/or disclosing personal information using facial analytics technology, via in-mall directories, without adequate consent. The technology, which CFCL referred to as Anonymous Video Analytics ("AVA") technology,[3] was installed on digital wayfinding directories, which are effectively touch screen digital map systems that allow visitors to locate stores and find their way through CFCL shopping malls. In the context of this report, AVA technology covers all elements of the software suite and hardware elements involved in CFCL's AVA implementation.

[4] Initial media reports[4] regarding CFCL's use of AVA technology in its directories surfaced in July 2018, after an individual posted a photo[5] on Reddit[6] taken at CFCL's Chinook Centre in Calgary, Alberta, showing a display screen with coding language that included "FaceEncoder" and "FaceAnalyzer" – leading the media to report that CFCL was using facial recognition technologies.

[5] Satisfied that reasonable grounds existed to investigate these matters, the Privacy Commissioner of Canada, Information and Privacy Commissioner for British Columbia and Information and Privacy Commissioner of Alberta each initiated investigations pursuant to s.11(2) of PIPEDA, s.36(1)(a) of PIPA BC, and s.36(1)(a) of PIPA AB, respectively. In August 2018, OIPC AB also received a complaint about CFCL. In December 2018, the Office of the Privacy Commissioner of Canada ("OPC"), the Office of the Information & Privacy Commissioner for British Columbia ("OIPC BC"), and the Office

[3] AVA technology generally refers to software designed to gather metrics about digital signage audience engagement. As described by the Ontario Information and Privacy Commissioner in a White Paper on AVA software, it generally operates by scanning "real-time feeds from video cameras utilizing pattern detection algorithms to identify shoppers anonymously for the purpose of creating aggregate reports".

[4] Sarah Rieger, "At least two malls are using facial recognition to track shoppers ages and genders without telling," *CBC*, Jul. 26, 2018.

[5] Facial Recognition Tech at Chinook?

[6] Reddit is an American social news aggregation, web content rating, and discussion website. Registered members submit content to the site such as links, text posts, and images, which are then voted up or down by other members (Wikipedia).

of the Information and Privacy Commissioner of Alberta (“OIPC AB”) decided to conduct the investigation jointly, at which time, the complaint received by OIPC AB was put in abeyance, pending the outcome of this joint investigation.

[6] In light of subsequent media reports[7] and information obtained during the preliminary stages of the investigation into CFCL’s deployment of the AVA technology, the scope of the joint investigation was expanded to determine whether CFCL obtained adequate consent for its collection, use, and disclosure of mall visitors’ personal information, including geolocation and Media Access Control (MAC)[8] address, via mobile device geolocation technologies. Further information discovered during the course of the investigation prompted us to also consider the retention of personal information obtained through the AVA technology.

[7] Finally, in light of the fact that the *Commission d’accès à l’information du Québec* (the “CAI”) was also examining the issue of AVA technology installed in CFCL shopping malls located in the Province of Quebec, the OPC, OIPC BC and OIPC AB entered a collaboration arrangement with the CAI in March 2019 in order to coordinate investigative efforts.

[7] Anis Heydari, “Cellphone tracking has been used in at least 1 Canadian mall, former employee says”, *CBC*, August 8, 2018.

[8] **M**edia **A**ccess **C**ontrol address is a 48-bit identification number embedded by manufacturers on every device’s network interface controller. The **MAC** address uniquely identifies each device on a network.

Methodology

[8] The investigative team sought representations and records relating to the possible collection, use or disclosure of personal information by CFCL with regard to both the AVA technology and geolocation technologies. These representations were sought from CFCL directly, as well as from the following third parties: (i) Mappedin, the third party service provider of the wayfinding directories (and AVA technology therein); and (ii) Aislelabs, the third party service provider for the geolocation technologies.

[9] After reviewing the initial representations from CFCL, the investigative team conducted a site visit at CFCL's headquarters in Toronto, Ontario, during which it interviewed key personnel and viewed CFCL's wayfinding directory in action, and the AVA technology therein. The investigative team also securely extracted records from the wayfinding directory for forensic analysis by the team's Technology Analysts.

[10] Subsequently, the investigative team also conducted a site visit at Mappedin's headquarters, during which it interviewed key personnel, and securely extracted records for forensic analysis by the team's Technology Analysts. Further, we obtained a copy of the database containing all of the data sent by the AVA technology installed in the wayfinding directories while the technology was operational. We note that this database was stored on a decommissioned server, and was not being used for production purposes.

[11] The investigation also included a visit to a CFCL property (CF Eaton Centre), with the specific goal of assessing CFCL customer service staff's ability to respond to basic customer privacy requests (e.g., provision of a copy of CFCL's privacy policy).

[12] Over the course of the investigation, we also considered the following material relied upon by CFCL:

i. CFCL provided a third-party analysis report (the "Third-Party Report") produced by an Associate Professor at the Faculty of Engineering at the Bar Ilan University in Israel ("the professor") whose research relates to high computer vision, machine learning, biometrics, and signal processing;

ii. A white paper titled Anonymous Video Analytics (AVA) technology and privacy,9 published by the Office of the Information and Privacy Commissioner of Ontario; and

iii. A white paper entitled Building Privacy Into Mobile Location Analytics (MLA) Through Privacy *by Design,*[10] published jointly by the Office of the Information and Privacy Commissioner of Ontario, and Aislelabs.

[9] White Paper: Anonymous Video Analytics (AVA) technology and privacy.

[10] Building Privacy into Mobile Location Analytics (MLA) *Through Privacy by Design*.

[13] Upon completion of our investigation, we issued a preliminary report of investigation to CFCL, which set out and explained the rationale for our preliminary conclusions and identified several recommendations. We then met with CFCL to address any questions or comments they had, and to discuss our recommendations. Subsequently, in its response to our preliminary report, CFCL committed to implement a number of our recommendations which would bring it into compliance with Canadian privacy laws. CFCL also provided further submissions and factual clarifications, which led our Offices to seek further commitments to ensure that CFCL would not contravene Canadian privacy laws through the future launch or reinstitution of practices similar to those examined in our investigation. CFCL refused to provide those commitments. All of the above is detailed in this final report.

[14] The investigation and findings focus on CFCL's legal obligations under the above-mentioned Acts. While this report examines the practices of certain third parties who provided services to CFCL, it does not draw any conclusions about the legal obligations of these parties, or any other organization or individual.

Issues

[15] The issues in this investigation are:

i. Whether CFCL’s use of the AVA technology, via wayfinding directories, resulted in the collection, use and/or disclosure of personal information; and if yes,

   a. Whether CFCL obtained adequate consent for that collection, use and/or disclosure; and
   b. Whether CFCL retained that information for longer than necessary; and

ii. Whether CFCL’s use of mobile device geolocation tracking technologies resulted in the collection, use and/or disclosure of personal information; and if yes, whether CFCL obtained adequate consent for that collection, use and/or disclosure.

CFCL’s Jurisdictional Challenge

AVA Technology

[16] At the outset of our investigation, and throughout its course, CFCL objected to our jurisdiction with respect to its use of the AVA technology, on the basis that the use of the technology did not result in the collection, use, or disclosure of personal information.

[17] In its representations, CFCL asserted that the information processed and gathered through the AVA technology was not personal information because it was anonymous, and in no way could it be used, alone or in combination with other information, to identify an individual. CFCL contended that all processing occurred locally and in real time, and at no time was an image, photograph or video created – except during testing and calibration, as covered at paragraph 54 of this report.

[18] CFCL explained that no attempt was made to obtain a positive identification of individuals within the visible field of view of the camera, and that the digital images were not matched against a database of known individuals.

[19] CFCL further represented that it was not engaged in the collection of personal information as defined by the Acts because nothing was “captured” by the AVA technology, and that “the absence of an ‘identifiable individual’ renders any ‘capture’ insufficient to qualify as collection of personal information”.

[20] Ultimately, after consideration of CFCL’s representations, and for the reasons outlined under “Issue 1” below, we determined that CFCL was collecting personal information via its AVA technology, such that we had jurisdiction to investigate this matter.

Geolocation Technology

[21] CFCL also objected to our Offices’ jurisdiction with respect to its use of geolocation technologies across its properties, on the basis that MAC addresses do not constitute personal information, and that the geolocation is about a device and not about an identifiable individual.

[22] In order to support its argument, CFCL drew a comparison with license plates on vehicles, and referred to the Alberta Court of Appeal’s decision in *Leon’s Furniture v. Alberta (Information and Privacy Commissioner)*.[11] CFCL asserted that MAC addresses are analogous to license plates:

> It is the mechanism that allows the vehicle to participate in the network of roads, it is visible and intended to be visible both to other vehicles and owners/operators of the roadways, and it is unique

[11] 2011 ABCA 94 [*Leon’s*].

> to that vehicle. Importantly, like a license plate, a MAC address is unique to a device, not an individual.

[23] In addition, CFCL further supported its position by referring to a past OPC case[12] wherein the OPC held that IP addresses[13] can constitute personal information if they can be associated with or linked to an identifiable individual.

[24] Our Offices considered CFCL's arguments as well as its representations, in determining whether CFCL did, in fact, collect personal information in the form of Wi-Fi triangulated geolocation data. As detailed under "Issue 2" below, our preliminary conclusion was that CFCL was collecting personal information via mobile-tracking technologies. However, subsequent to the issuance of our preliminary report, based on clarifications from CFCL and Aislelabs, we determined this not to be the case.

[12] PIPEDA Report of Findings #2009-010

[13] An **I**nternet **P**rotocol address is a numerical label assigned to a device when it connects to a network. The **IP** address identifies the device and routes its network traffic.

Issue 1: Whether CFCL's use of the AVA technology, via in-mall directories, resulted in the collection, use and/or disclosure of personal information, and if yes, whether CFCL obtained adequate consent for the collection, use and/or disclosure; and whether CFCL retained such information longer than necessary

CFCL Representations and our Investigation

Overview of CFCL's AVA Implementation

[25] CFCL contracted with a third-party company, Mappedin, to provide CFCL with software and support services for interactive digital wayfinding directories, which CFCL installed in many of its retail properties across Canada. Mappedin describes itself as providing an indoor geographical information system. The organization works with nine out of ten of the largest malls in Canada, including some owned by CFCL, and claims that it seeks to help make the indoors more discoverable in stores, hospitals, campuses, and airports around the world. Additional related services under the contract with CFCL include map design, user experience development, and ongoing support and hosting.

[26] The wayfinding directories all contained optical devices (i.e., cameras) behind protective glass on the periphery of the screen, such that they were not easily noticeable. The cameras were non-operational when first installed because they were not supported by underlying software. CFCL advised that AVA technology, consisting of a particular software package, was first installed by Mappedin on June 13, 2017 on a test basis, and then disabled and removed on December 1, 2017, ("Testing Period"). The AVA technology was subsequently rolled out in 12 malls across Canada (roughly 60% of directories) between May 31 2018 and July 31 2018.[14] CFCL indicated that they considered this implementation to be a "pilot project". The AVA technology was operational in wayfinding directories in the following shopping malls:

Property	Province
CF Market Mall	Alberta
CF Chinook Centre	Alberta
CF Richmond Centre	British Columbia
CF Pacific Centre	British Columbia
CF Polo Park	Manitoba

[14] While CFCL represented that it ceased use of the AVA technology on July 31 2018, we note that in the course of our investigation we identified information collected from AVA on Mappedin's servers bearing timestamps up to August 03 2018.

CF Toronto Eaton Centre	Ontario
CF Sherway Gardens	Ontario
CF Lime Ridge	Ontario
CF Fairview Mall	Ontario
CF Markville Mall	Ontario
CF Galeries d'Anjou	Quebec
CF Carrefour Laval	Quebec

[27] According to CFCL, during the initial testing and calibration period (as described in paragraph 54), and between May 2018 and July 2018, when the AVA technology was operational, the technology generated data, which was then sent for analysis by Mappedin, which provided CFCL with anonymous, aggregate insights into traffic patterns and directory use.

Further details regarding Mappedin

[28] According to the latest Master Agreement (the "Agreement") between CFCL and Mappedin, dated July 20, 2017, all information provided by CFCL remained CFCL's sole and exclusive property. It further provided that all data produced under the Agreement was shared property between CFCL and Mappedin, and licensed to CFCL for use and distribution to any third party by CFCL (except under the circumstance where such third party was deemed by Mappedin as a competitor). We note that while the Agreement did mention the integration of webcams, it did not make any reference to the AVA technology. Nevertheless, based on the terms of the Agreement, we understand that CFCL remained responsible for information collected by Mappedin on its behalf.

[29] In representations to our offices, Mappedin advised that it does not use the information obtained in the context of the Agreement for any purposes other than to provide the contracted services. Mappedin further stated that it does not share, and has not shared any such information with third parties.

The AVA Technology

[30] In its representations to the investigative team, CFCL described the AVA technology as "facial detection software". It stated that the AVA technology assessed objects coming into the field of view of the camera in real time to determine if there was a human face present. If the underlying software detected a human face present, the software would then produce assessments of the probable gender and age range for that face. CFCL stressed in its submissions that at no time was the AVA technology capturing images or any other personal information since the gender and age range outputs were anonymous, and that "[n]o information other than the anonymous output data is retained."

[31] As noted in paragraph 12, during the course of the investigation, CFCL retained the professor to conduct a study of the AVA technology for the investigative team's consideration. The Third-Party Report was provided to us following the initial site visit. CFCL has maintained that the AVA technology did not have any facial recognition capabilities; however the report contradicts this assertion to the extent that it references the use of a software called FaceNet, which is "facial recognition" software.

[32] Following our receipt of the Third-Party Report, we reached out to the professor in order to seek more information with regard to the methodology used to conduct the analysis found in the report.

[33] The professor indicated that his opinion was based on the following materials provided by CFCL's external legal representatives:

i. A "snapshot" of the AVA technology (consisting of parts of the programming code);
ii. A copy of the "Notification of Site Visit" issued to CFCL by the OPC;
iii. The Notice of Joint Investigation issued to CFCL by the OPC, OIPC BC and OIPC AB; and
iv. A copy of a letter provided to the OPC by CFCL, responding to questions posed by the investigative team in the course of the investigation.

[34] In the Third-Party Report, the professor made the following conclusions:

> It is my opinion that the AVA software does not report any personal information of the customers. The stored gender and coarse age estimates generated by the system are anonymous and cannot be tracked back to a particular customer.

[35] Despite the conclusions of the Third-Party Report, our investigation determined that the AVA technology in question operated differently than initially represented by CFCL, and that it indeed resulted in the collection of personal information, as detailed below.

[36] We established that the AVA technology performs a number of sequential steps in generating and collecting demographic information, from image input to demographic output (age and gender estimation). These steps are, as referred to in the Third-Party Report submitted by CFCL: (i) face detection; (ii) face encoding; and (iii) face tracking.

[37] CFCL's initial representations stated that the AVA technology relied on an open-source software called Rude Carnie[15] in order to generate age and gender estimations. The developers of that software describe the purpose of the software as being able to "[d]o face detection and age and gender classification on pictures".

[15] Rude Carnie: Age and Gender Deep Learning with TensorFlow.

[38] After reviewing the records extracted during our site visit at CFCL's headquarters, we learned that the AVA technology employed another software[16] named FaceNet, described as a "face recognizer". As noted in paragraph 31, this was confirmed in our subsequent review of the Third-Party Report. On the software's webpage, a research paper[17] provides an in-depth review of the software, describing it as being a "unified system for face verification (is this the same person), recognition (who is this person) and clustering (find common people among these faces)".

Face detection and tracking

[39] Our investigation confirmed that the first step undertaken by the AVA technology was facial detection. The technology was trained to detect the visual formation of one or more human faces within the field of view of the camera installed in the wayfinding directory.

[40] Once the technology detected what it assessed to be a human face, it generated a bounding box around the face, and captured the image therein for conversion and processing. This "capture" resulted in an actual digital image – or photograph – of the face being retained for a period of a few milliseconds. We do note that, save for the testing and calibration period (see paragraph 54), no persistent image was retained after this processing.

[41] Our investigation further revealed that during the detection process, the technology also has the ability to, and does, differentiate faces from one another should there be more than one face in the field of view of the camera. In order to do so, the technology attributed a unique identifier, a random number, to each face detected.

[42] Mappedin represented that the software was capable of assigning a unique identifier ("unique identifier") to each face present in the field of view; however, they indicated that these unique identifiers were "randomly assigned" and "non-identifying". Both Mappedin and CFCL indicated that this feature was only in place so that the AVA technology could track and differentiate individual faces within the field of view of the camera. As such, should a user exit the field of view and subsequently return, the AVA technology would assign a new random unique identifier. An example of one such unique identifier can be found in the screen capture at paragraph 53 (referenced as "id").

[43] Contrary to representations from CFCL stating that only the age and gender demographic information was retained, in the course of our investigation, we discovered that Mappedin, on behalf of CFCL, collected and retained these unique identifiers in its database, along with additional information associated therewith

[16] Face Recognition using TensorFlow.

[17] Florian Schroff, Dmitry Kalenichenko, James Philbin, FaceNet: A Unified Embedding for Face Recognition and Clustering (2015).

(including, most importantly, numerical representations of individual faces captured - see paragraphs 44 & 53 of this report). When asked the purpose for such collection, Mappedin was unable to provide a response, indicating that the person responsible for programming the code no longer worked for the company.

Face encoding and embedding

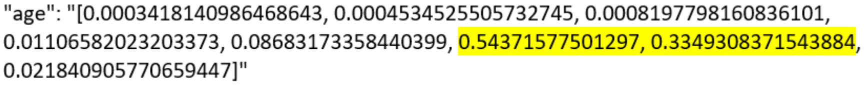
[44] In order for the technology to differentiate and track individual faces interacting with a wayfinding directory, the AVA technology converted and encoded the captured images, which involved the computation of a series of measurements of each face. This process generated a numerical representation, through an embedding process, of each detected face. Once this process was complete, the captured images of faces were overwritten.

Age and gender estimation

[45] Our investigation confirmed that as the captured images are processed, the AVA technology estimates the probability that the face in question falls into each of eight pre-defined age groups. These are:

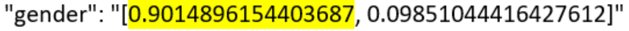
0-2	4-6	8-12	15-20	25-32	38-43	48-53	60-100
1	2	3	4	5	6	7	8

[46] The assessment captures these probabilities in the form of numerical values. As the sample output below demonstrates, the technology made the determination that there is a significantly higher probability that the subject would fall into age group number 6 (38-43) or 7 (48-53) than any of the other groups:



```
"age": "[0.0003418140986468643, 0.0004534525505732745, 0.0008197798160836101,
0.01106582023203373, 0.08683173358440399, 0.54371577501297, 0.3349308371543884,
0.021840905770659447]"
```

[47] A similar assessment process occurs for gender estimation, though the values are divided between binary options: male or female. In the sample output below, the AVA technology determined that there was a 90% probability of the face being the first binary option (male):



```
"gender": "[0.9014896154403687, 0.09851044416427612]"
```

[48] CFCL and Mappedin both represented that the entirety of the age and gender estimation process summarized above occurs in milliseconds and that each image of a face is only stored in computer memory for the duration of that process. Our investigation confirmed that assertion. However, as noted in paragraph 50, additional information was collected and used in conjunction with the processing of the images.

Additional information sent to Mappedin

[49] As previously mentioned, CFCL represented that the only information collected and retained through the deployment of the AVA technology was anonymous demographic information. It further provided that Mappedin "simply" analyzed the demographic information to provide CFCL with "anonymous, aggregate insights into traffic patterns and directory usage." However, as outlined above, our investigation discovered that Mappedin, on behalf of CFCL, collected, used and retained significantly more information than CFCL originally indicated to the investigative team.

[50] Our forensic analysis of the data extracted from the wayfinding directory during the CFCL site visit revealed that in addition to the demographic information (age and gender), the AVA technology was collecting and/or generating the following information in respect of each face detection event, which was pushed to the Mappedin servers where it was retained on behalf of CFCL:

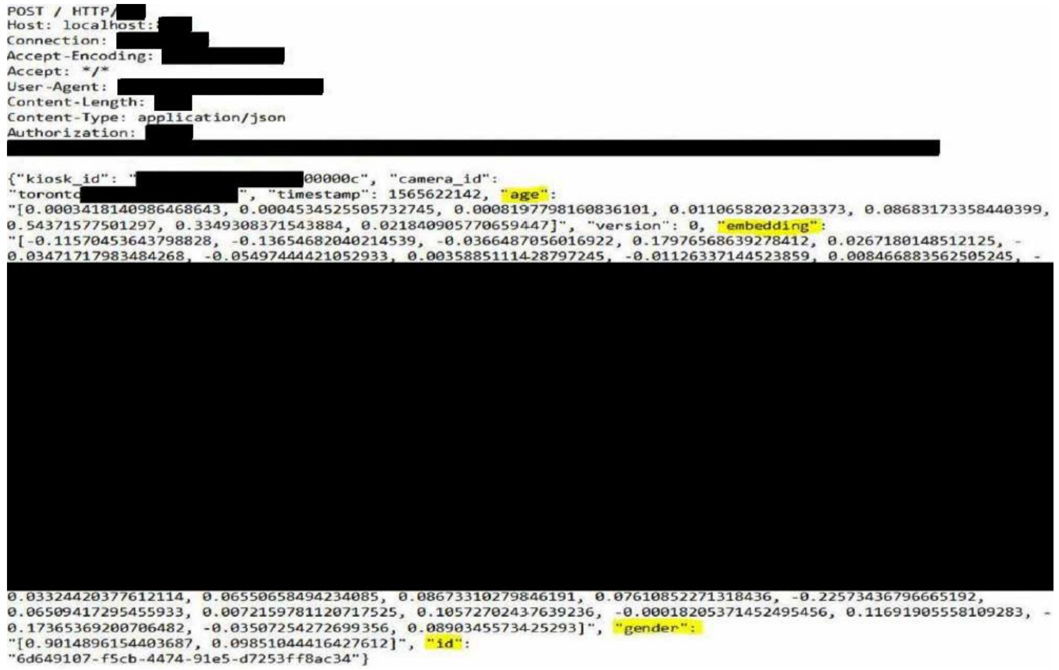
i. A unique identifier for the wayfinding directory in which the collection occurred;
ii. A unique identifier for the camera used for the collection;
iii. A unique identifier for tracking and differentiating faces in the field of view;
iv. A numerical representation of individual faces;
v. The property in which the camera is located; and
vi. A timestamp.

[51] Following the site visit, we obtained from Mappedin the database of all information it collected, used and retained on behalf of CFCL in relation to the AVA technology. Through forensic analysis of the database, we further confirmed that CFCL, via Mappedin, had been collecting, using and retaining more than the age and gender estimation.

[52] In total, for the period during which the AVA technology was operating, CFCL, via the AVA technology, collected, used and retained **5,061,324** numerical representations of faces, from an unknown number of individuals.

[53] Below is a screen capture[18] of the information collected and retained in Mappedin's database for a single face processed by the AVA technology:

[18] Portions of data have been redacted for anonymization purposes, namely: the kiosk and camera identifier pointing to a specific location, authorization code, and some numerical facial representation values (which are in the same format as the values above and below the redaction). Highlighting added for ease of reference.



```
POST / HTTP/[redacted]
Host: localhost:[redacted]
Connection: [redacted]
Accept-Encoding: [redacted]
Accept: */*
User-Agent: [redacted]
Content-Length: [redacted]
Content-Type: application/json
Authorization: [redacted]

{"kiosk_id": "[redacted]00000c", "camera_id":
"toronto[redacted]", "timestamp": 1565622142, "age":
"[0.0003418140986468643, 0.0004534525505732745, 0.0008197798160836101, 0.01106582023203373, 0.08683173358440399,
0.54371577501297, 0.3349308371543884, 0.021840905770659447]", "version": 0, "embedding":
"[-0.11570453643798828, -0.13654682040214539, -0.0366487056016922, 0.17976568639278412, 0.0267180148512125, -
0.03471717983484268, -0.05497444421052933, 0.003588511428797245, -0.01126337144523859, 0.008466883562505245, -
[redacted]
0.03324420377612114, 0.06550658494234085, 0.08673310279846191, 0.07610852271318436, -0.22573436796665192,
0.06509417295455933, 0.007215978112071 7525, 0.10572702437639236, -0.00018205371452495456, 0.11691905558109283, -
0.17365369200706482, -0.03507254272699356, 0.08903455734 25293]", "gender":
"[0.9014896154403687, 0.09851044416427612]", "id":
"6d649107-f5cb-4474-91e5-d7253ff8ac34"}
```

Information Collected During the Testing and Calibration Period

[54] CFCL advised us that a testing and calibration exercise was undertaken before it deployed the AVA technology. Specifically, CFCL ran the calibration exercise at the CF Toronto Eaton Centre and CF Sherway Gardens, both located in Ontario, on April 29, May 12 and May 13, 2018 ("Calibration Period"). The Calibration Period generated sixteen one-hour videos, which Mappedin retained on behalf of CFCL.

[55] We note that during our analysis of the videos, we found that in three of the sixteen videos, the audio function had been enabled, which resulted in yet another dimension to the collection, use and retention of personal information via audio recordings.

CFCL's Privacy Communications regarding AVA

[56] Notwithstanding the evidence revealed through this investigation, CFCL took the position that since it was not, in its view, collecting personal information via the AVA technology, other than during the testing and calibration period, it was not required to provide notice to its customers regarding the practice.

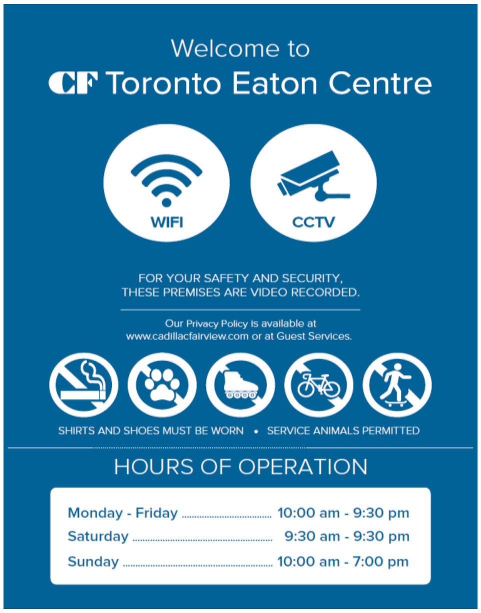
[57] We asked CFCL if it had taken any measures to inform individuals that it was conducting testing of the AVA technology, to which CFCL represented: "to the extent any personal information was collected during the testing phase, this is clearly set out CFCL's Privacy Policy…".[19]

[19] The CFCL Privacy Policy in effect during this investigation was available on this page. An archived copy of this Privacy Policy can be found here.

[58] CFCL then referred to a passage in its Privacy Policy (last updated July 20, 2016) that reads as follows:

> 2. IDENTIFYING PURPOSES
>
> "We collect personal information that is relevant for the purposes of providing services to our guests, service providers and clients (which includes retailers and occupants of our properties); securing our properties, websites and mobile applications; meeting our legal obligations; promoting, advertising and marketing our services and, in some cases, the products and services of our clients; and researching and developing new products and techniques to improve our services, business, our properties, websites, and mobile applications."
>
> […]
>
> WHAT TYPES OF PERSONAL INFORMATION DO YOU COLLECT AND USE?
>
> "Some of our properties are also equipped with technologies such as ibeacons (sensors) and cameras that we use to monitor foot traffic patterns and may that may [sic] assist us in predicting demographic information about our visitors during your visit to our properties."

[59] CFCL further stated that decals on the entrance doors of all shopping malls directed guests to CFCL's Privacy Policy should they want more information on CFCL's practices. We note that, as displayed in the figure below, installed at the CF Toronto Eaton Centre from May to June 2018, the only stated purposes of video recording are for "safety and security".



Welcome to
CF Toronto Eaton Centre

FOR YOUR SAFETY AND SECURITY,
THESE PREMISES ARE VIDEO RECORDED.

Our Privacy Policy is available at
www.cadillacfairview.com or at Guest Services.

SHIRTS AND SHOES MUST BE WORN • SERVICE ANIMALS PERMITTED

HOURS OF OPERATION

Monday - Friday	10:00 am - 9:30 pm
Saturday	9:30 am - 9:30 pm
Sunday	10:00 am - 7:00 pm

Analysis

Was there Collection, Use and/or Disclosure of Personal Information?

[60] In our view, CFCL clearly did collect and use, via the AVA technology, personal information, as defined in the Acts, including: captured images of faces, the numerical representation assigned to each face and the assessment of age range and gender. CFCL disagrees with this finding. We also note that while CFCL collected and used numerical representations of faces suitable for facial recognition, we found no evidence that it sought to, or did, use these representations for the specific purpose of identifying individuals.

[61] Subsection 2(1) of PIPEDA, section 1 of PIPA BC and paragraph 1(1)(k) of PIPA AB all define personal information as information about an identifiable individual. Courts have found in various cases that personal information must be given a broad interpretation as to give effect to the legislation's intended purpose.[20] Courts have also found that information will be considered personal where it is reasonable to expect that a person can be identified from the information at issue when combined with information from sources otherwise available.[21]

[62] We do not accept CFCL's assertion that the AVA technology worked entirely in real-time. Rather, the captured images of individual faces coming into the field of view of the cameras were kept in memory, albeit for a very short period of time, while the technology processed these images, with the resulting information and analyses to be used thereafter.

[63] The images of individual faces captured by the AVA technology through the cameras installed on the wayfinding directories are, in and of themselves, clearly personal information. Past cases have consistently found that images or photographs of individuals can and do constitute personal information under PIPEDA,[22] PIPA BC[23] and PIPA AB.[24] As such, while we agree that the captured images were held in memory for a very short period, that practice did represent a collection of personal information.

[64] Moreover, our investigation found that the images captured by the technology were used to generate additional personal information including numerical representations,

[20] *Dagg v. Canada (Minister of Finance)*, [1997] 2 S.C.R. 403, dissenting, at para 68; *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157.

[21] *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157; Girao v. Zarek Taylor Grossman Hanrahan LLP, 2011 FC 1070 para 32.

[22] *See, e.g.* PIPEDA Case Summary 2002-53; PIPEDA Case Summary 2008-392; PIPEDA Case Summary 2002-89; PIPEDA Report of Findings 2013-016; PIPEDA Case Summary 2008-396.

[23] *See, e.g.* Order P09-02 from the OIPC BC.

[24] *See, e.g.* Orders P2009-013 and P2009-014 from OIPC AB.

age range and gender of individual faces, which were then collected and retained for a much longer time period.

[65] In particular, we are of the view that the embedding process, which results in the creation of a unique numerical representation of a particular face, constitutes a collection of biometric[25] information, because that information is uniquely derived from a particular identifiable individual, and could be used, and is used in the context of the AVA technology in this case, to distinguish between different individuals. Based on CFCL and Mappedin's representations regarding the use of FaceNet software to detect and differentiate faces during the collection process, we have determined that these numerical representations are created by FaceNet to identify a number of facial features, which would normally enable the software to recognize specific individuals.[26] We do note that consistent with CFCL's and Mappedin's representations, we found no evidence that either were using the technology for the purpose of identifying individuals. Nonetheless, the collection, use and retention of approximately **5 million** such numerical representations, which we view as sensitive personal information, occurred via the AVA technology.

[66] As stipulated by the courts, information will be about identifiable individuals when the information in question, together with other available information would tend to or possibly identify them.[27] "About" is also defined as being information that is not just the subject of something but also relates to or concerns the subject – such as images and/or biometric information.[28] In that regard, previous Alberta investigations have found biometric information to be personal information.[29] Similarly, OPC's guidance on biometrics,[30] and past investigations, clearly affirm that biometric information is personal.[31]

[25] As stated on OPC webpage resource, "Data at Your Fingertips Biometrics and the Challenges to Privacy":

> Originally, the word "biometrics" meant applying mathematical measurements to biology. 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.

[26] Florian Schroff, Dmitry Kalenichenko, James Philbin, FaceNet: A Unified Embedding for Face Recognition and Clustering (2015).

[27] *Gordon v. Canada (Health)*, 2008 FC 258 ; Girao v. Zarek Taylor Grossman Hanrahan LLP, 2011 FC 1070 para 32.

[28] *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157.

[29] *See, e.g.* Investigation reports F2008-IR-001 and P2008-IR-005.

[30] OPC, "Data at Your Fingertips Biometrics and the Challenges to Privacy", (2011).

[31]*See, e.g.* PIPEDA Case Summary #2010-007, PIPEDA Case Summary #2004-281.

[67] The England and Wales High Court of Justice recently held that biometric data, in the form of numerical representations of faces, enables the unique identification of individuals with some accuracy, which is what distinguishes it from other forms of data.[32] As the court stated:

> Like fingerprints and DNA, AFR [Automated Facial Recognition] technology enables the extraction of unique information and identifiers about an individual allowing his or her identification with precision in a wide range of circumstances. Taken alone or together with other recorded metadata, AFR-derived biometric data is an important source of personal information. Like fingerprints and DNA… it is information of an “intrinsically private” character. The fact that the biometric data is derived from a person’s facial features that are “manifest in public” does not detract from this. The unique whorls and ridges on a person’s fingertips are observable to the naked eye. But this does not render a fingerprint any the less a unique and precise identifier of an individual. The facial biometric identifiers too, are precise and unique [emphasis in original document].[33]

[68] Additionally, given that the numerical representations of individual faces were created from images already captured by the AVA technology, we are also of the view that the creation of such biometric information from the images constituted a distinct and additional collection and use of personal information regardless of the fact that the original images were not retained.

[69] With respect to the White Paper referenced at paragraph 12 of this report, for the following reasons, we cannot accept CFCL’s submission that the paper supports the assertion that CFCL’s AVA technology did not violate PIPEDA, in that no personal information was “recorded” (other than during the testing and calibration period):

i. First, we note that the White Paper was prepared in the context of Ontario’s *Freedom of Information and Protection of Privacy Act* (“FIPPA”). Subsection 2(1) of that legislation defines “personal information” as “recorded information about an identifiable individual”, while paragraph 2(1)(a) defines “record” as “any record of information however recorded, whether in printed form, on film, by electronic means or otherwise”, including “a photograph”. PIPEDA, PIPA BC and PIPA AB, however, define “personal information” differently, and do not require the information to be “recorded” to constitute personal information. Therefore, compliance with these Acts cannot be resolved by reference to a report prepared in a different legislative context.

ii. Furthermore, in our view, as outlined above, personal information is “recorded” by the AVA technology in this case, since digital images must be temporarily captured in order for the technology to process them, and then further biometric and other data is derived from those images and retained. As a result, whether realized through a photo or a set of data-points, the characteristics of a face are being recorded.

[32] *R (Bridges) v. CCSWP and SSHD*, [2019] EWHC 2341 (Admin) [UK Decision].

[33] *Ibid*. at para. 57.

[70] We also do not accept CFCL's assertion that the *Morgan v Alta Flights Inc.* decision[34] has any application to the facts presented here. That case dealt with a tape recorder that was installed by an employer to make audio recordings of its employees, but the recorder in fact failed to record audio. On that basis, the court held that because the conversation was not actually recorded, there was no collection as understood by PIPEDA in that case. However, neither the Federal Court or Federal Court of Appeal stated that personal information must, in all cases, be recorded in order to constitute a collection under PIPEDA or other private-sector privacy legislation. Furthermore, as our investigation has established, the AVA technology did in fact "record", and in our view collect, personal information in the form of images and biometrics.

[71] We accept that the demographic output generated by the AVA technology, such as age and gender assessments, would not, on their own, constitute personal information for the purposes of the Acts. That said, non-identifying information can be "personal information" in context,[35] and in this case, the demographic output was retained with other information including unique biometric information, location, and a timestamp. It is our view that the combination of this information raises a likelihood, beyond a "serious possibility", that the individual could be identified. This is the case even though we found no evidence that CFCL attempted to identify individuals from this collected personal information. It is therefore our position that the demographic output also constitutes personal information in this context.

[72] As such, we cannot accept the conclusions from the Third-Party Report that the "stored gender and coarse age estimates generated by the system are anonymous". The methodology of that report was limited and failed to take into account the extensive information that had been collected and generated by CFCL, which we were able to obtain in the course of our investigation.

[73] Finally, we are of the view that the collection of video and audio recordings during the calibration and testing period also constitutes a collection of personal information pursuant to the Acts.

Was there Valid Consent and Notice?

[74] CFCL did not ensure valid consent and notice, for its collection and use of personal information via the AVA software, as detailed above. In coming to this determination, our Offices considered: (i) the appropriate form of consent for CFCL's practice; (ii) the meaningfulness of consent in the context at hand; and (iii) the adequacy of the notice provided by CFCL for the purposes of PIPEDA, PIPA AB and PIPA BC.

[34] *Morgan v. Alta Flights Inc.* (2006) FCA 121, affirming (2005) FC 421

[35] *Gordon v. Canada (Health)*, 2008 FC 258 ; *See e.g,* Order P-12-01 from the Office of the Information and Privacy Commissioner for British Columbia.

[75] Principle 4.3 of Schedule 1 of PIPEDA states that the **knowledge** and **consent** of the individual is required for the collection, use, or disclosure of personal information, unless these requirements are specifically exempted under section 7 of PIPEDA. Principle 4.3.4 further provides that the form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. Although some information (for example, medical records and income records) is almost always considered to be sensitive, any information can be sensitive, depending on the context. Principle 4.3.5 provides, in part, that in obtaining consent, the reasonable expectations of the individual are also relevant. Finally, Principle 4.3.6 states that the way in which an organization seeks consent may vary, depending on the circumstances and the type of information collected. An organization should generally seek express consent when the information is likely to be considered sensitive.

[76] Similarly, section 7(1) of PIPA AB requires the consent of the individual for the collection, use, or disclosure of personal information, except where the Act specifies. Section 8 of PIPA AB sets out the various forms of consent, which include the following three possibilities:

i. express oral or written consent;
ii. deemed consent where it is reasonable that an individual would voluntarily provide the information for a particular purpose; and
iii. 'opt-out' consent where the organization must provide easy-to-understand notice to the individual of the particular purposes of the collection, use or disclosure, the individual has a reasonable opportunity to decline or object, and opt-out consent is appropriate for the level of sensitivity of the personal information involved.

[77] PIPA BC contains similar requirements to the above. In line with section 6 of PIPA BC, consent for the collection, use or disclosure of personal information is required unless an exemption is specifically authorized by the Act. Subsection 7(1) of PIPA BC states that an individual has not consented unless they have been given notice. In consideration of express versus implied consent, section 8(1) of PIPA BC sets out the criteria under which deemed consent for the collection, use or disclosure of personal information is applicable.

[78] The *Guidelines for obtaining meaningful consent*[36] (the "Guidelines") jointly issued by the OPC, OIPC AB and OIPC BC provide that "organizations must generally obtain *express* consent" when: (i) the information being collected, used or disclosed is sensitive; (ii) the collection, use or disclosure is outside of the reasonable expectations of the individual; and/or (iii) the collection, use or disclosure creates a meaningful

[36] Guidelines for obtaining meaningful consent (2018).

residual risk of significant harm. This is reinforced by a decision made by the Supreme Court of Canada.[37]

[79] In our view, biometric information is sensitive in almost all circumstances. It is intrinsically, and in most instances permanently, linked to the individual. It is distinctive, stable over time, difficult to change and largely unique to the individual. Within the category of biometric information, there are degrees of sensitivity. Facial biometric information is more sensitive since possession of a facial recognition template can allow for identification of an individual through comparison against a vast array of images readily available on the internet or via surreptitious surveillance.

[80] Furthermore, mall visitors would not, in our view, reasonably expect CFCL's collection and use of their biometric information. In fact, a visitor would have no reason to expect that their image was being collected by an inconspicuous camera while searching a mall directory. Nor would such an individual expect that this image would be used to create a biometric representation in support of CFCL's commercial analytics.

[81] As such, in order to comply with the Acts, and conduct its practices in accordance with the Guidelines as reinforced by the Supreme Court of Canada, CFCL should have obtained express opt-in consent. That consent should have been obtained at the time of the visitor's engagement with the map, before CFCL captured and processed their image via the AVA technology.

[82] Secondly, we cannot accept CFCL's reference to its Privacy Policy as supporting meaningful consent to the collection and use of personal information via the AVA technology, whether for the video and audio recordings collected and used for calibration and testing, or for the subsequent collection and use primarily at issue.

[83] Principle 4.3.2 of Schedule 1 of PIPEDA provides that an organization must make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used and to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. In addition, section 6.1 of PIPEDA requires that for consent to be valid, it must be reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use, or disclosure of the personal information to which they are consenting.

[84] Section 13(1) of PIPA AB requires that before or at the time of collecting the individual's personal information from the individual, the organization must notify the individual in writing or orally of the purposes for which the information is collected. The notice must

[37] *Royal Bank of Canada v. Trang*, 2016 SCC 50 paras 23 & 34

also include the name, position, or title of a person who is able to answer on behalf of the organization the individual’s questions about the collection.

[85] Section 10(1) of PIPA BC requires that on or before collecting personal information about an individual from the individual, an organization must disclose to the individual verbally or in writing the purposes for the collection of the information. The organization must, upon request, also provide the position name or title and the contact information for an officer or employee of the organization who is able to answer the individual's questions about the collection.

[86] Additionally, the Guidelines provide that individuals should be made aware of all purposes for which information is collected, used or disclosed. These purposes must be described in meaningful language, avoiding vagueness like ‘service improvement’, and should not be buried in a Privacy Policy or terms of use as it serves no practical purpose to individuals with limited time and energy to devote to reviewing privacy information. [emphasis added]

[87] In this case, individuals would not have understood the nature of the practices in question as they had not been notified, and were otherwise unaware, that CFCL was using the AVA technology. While CFCL’s Privacy Policy states that some of its properties are equipped with cameras that it uses to “monitor foot traffic patterns and [that may] assist [CFCL] in predicting demographic information” about mall visitors, and that personal information may be collected for the purpose of “researching, developing new products and techniques to improve its services”, these statements would not have allowed those mall visitors to reasonably understand that while they were using a mall directory: (i) close-range video and audio recordings were being taken of them during the testing and calibration period; and/or (ii) that their faces were being detected, captured in the form of digital images, and turned into numerical representations by facial recognition software for the purposes of predicting demographic information about them, such as their age range and gender. We also note that this information is embedded approximately 2,300 words into a 5,000-word Privacy Policy, which many users will never read before their image is captured.

[88] Similarly, CFCL could not rely on the decals installed on mall entrances as sufficient to ensure adequate consent under PIPEDA; nor do they constitute adequate notice under PIPA AB or PIPA BC. As shown at paragraph 59 of this report, the decal only mentions that video recordings are for visitor “safety and security”, and does not indicate any other purposes, such as those associated with CFCL’s use of the AVA technology. Further, the link provided is a link to CFCL’s website homepage, not the actual Privacy Policy. There is no indication that video recordings or cameras are used for any purpose other than “safety and security”, and the wayfinding cameras are inconspicuous in comparison to the more obvious security cameras, such that there is no evident reason or prompt for visitors to search out further information about further uses in a privacy

policy. These other uses, which are of a less intuitive and more questionable nature, are in fact conspicuous in their absence from the signage.

[89] Moreover, the Guidelines provide that in order for consent to be considered valid, or meaningful, organizations must inform individuals of their privacy practices in a comprehensive and understandable manner. This means that organizations must provide information about their privacy management practices in a form that is readily accessible [emphasis added]. We note that CFCL's wayfinding directories are physical locations, while their referenced Privacy Policy is available on their website, or at Guest Services elsewhere in the mall. Thus, the Privacy Policy is not readily accessible to individuals while they are engaging with a wayfinding map.

[90] Furthermore, given that mall visitors would be unaware of the AVA technology, or even alerted that video recordings may be used for purposes beyond safety and security, they would have no reason to seek out the Privacy Policy to obtain further information, and it would not be intuitive for them to seek out an online policy to understand privacy practices in a physical shopping environment.

[91] We further note that with regard to the accessibility of CFCL's Privacy Policy, we attempted, in the course of the investigation, to obtain a copy of CFCL's Privacy Policy at its Toronto Eaton Centre's Guest Service Desk. We noted that the employee seemed confused about the request, and indicated that they did not have a copy of the Privacy Policy. It was only after returning a second time, and additional prompting, that the employee offered to print a copy of the Privacy Policy, which in fact, turned out to be CFCL's ''privacy statement'' as opposed to the entirety of the policy.

[92] To conclude on the question of meaningfulness, it is our view that for the consent to have been meaningful, it should have been supported by a clear and conspicuous explanation of the purposes for which CFCL would capture and use individuals' personal information, as well as what information would be collected and how it would be used. CFCL provided no such explanation to wayfinding directory users and did not obtain meaningful consent for its AVA practices.

Was Personal Information Retained appropriately?

[93] As noted in paragraph 52 of this report, during the course of the investigation, our Offices discovered that Mappedin retained, on CFCL's behalf, **5,061,324 numerical representations of faces** and associated information. Given that no purpose for such retention could be identified or explained, our Offices made the decision to expand the scope of the investigation to consider whether CFCL met its obligations pursuant to the provisions of the Acts pertaining to the retention of personal information.

[94] As previously established, our Offices consider these numerical representations and associated information to be personal information within the meaning of the Acts. We note that principle 4.5.3 of PIPEDA, section 35 of PIPA AB and section 35 of PIPA BC all

set out requirements to destroy or depersonalize any personal information when it is no longer needed to fulfill the identified purpose of its collection, or in the case of PIPA BC, one year subsequent to being used to make a decision. We note that when asked, Mappedin could not articulate any purpose for the collection or retention of this information on behalf of CFCL. As such, in addition to the fact that CFCL did not obtain valid consent to collect the original images, CFCL and MappedIn had no identified reason to retain these numerical representations, beyond the very brief period necessary for the AVA software to process the images. While we acknowledge Mappedin's claim that the server containing the information had been "decommissioned", this did not in our opinion, meet the requirements of the Acts, as the server was readily re-activated with all personal information accessible. In fact, we have found in breach investigations[38] that legacy systems and "decommissioned" data, if not deleted, can quickly find their way into nefarious hands should a cyber attack occur.

[95] Consequently, we find that CFCL contravened: principle 4.5.3 of Schedule 1 of PIPEDA; section 35 of PIPA AB; and section 35 of PIPA BC.

Recommendations

[96] In our preliminary report, we recommended that if CFCL decides to pursue the use of the AVA technology in its shopping malls, it should obtain express opt-in consent, in accordance with the Acts and consistent with the *Guidelines for obtaining meaningful consent*. CFCL could, for example, undertake to implement changes to the way visitors interact with wayfinding directories by prompting a message box on the screen as soon as one or more faces are detected. The message should explain, in a simple and comprehensible way, the privacy implications associated with the AVA technology – including the collection and use of biometric information. Users should have the option to opt-in or refuse to provide consent, and should not be required to consent, as a condition to being able to use the wayfinding directory.

[97] Alternatively, we recommended that CFCL cease the use of the AVA technology.

[98] In addition to the above, our Offices recommended that CFCL ensure that all facial arrays (i.e., numerical representations) and associated information are deleted, as they were collected without consent and retained for no discernable purpose.

[99] Finally, our Offices recommended that CFCL ensure that frontline staff are trained and kept apprised of their obligation to provide the entirety of the Privacy Policy upon request at service desks.

[38] See e.g., Investigation into Equifax Inc. And Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach of personal information.

CFCL’s Response to our Recommendations

Consent

[100] CFCL expressly disagreed with our findings. Nevertheless, it confirmed that it had disabled its AVA software on July 31, 2018 and subsequently removed the technology from its wayfinding kiosks, and that it had no current plans to reinstall the technology.

[101] CFCL also agreed to engage front-line staff in a training program that would help ensure that they are kept apprised of their obligation to provide the entirety of the Privacy Policy upon request at service desks. CFCL advised that this training was completed on July 30th 2020, and that yearly refresher training would be provided.

[102] We noted that CFCL’s commitments did not preclude the possibility of reimplementing its AVA program in future. We therefore asked CFCL to confirm that should it do so, it would obtain consent consistent with our Offices’ recommendation, as outlined in paragraph 96 above.

[103] CFCL responded that if in the future it were to pursue the use of the AVA technology in its shopping malls, it would obtain “adequate consent, in accordance with the applicable privacy legislation and consistent with the *Guidelines for obtaining meaningful consent”*.

[104] CFCL refused, however, to commit to obtaining consent consistent with our recommendations (i.e., to obtain express opt-in consent), asserting that our recommendation was speculative.

Retention

[105] CFCL has confirmed to us that it has deleted the numerical representations and associated information and any calibration videos in its custody or under its control that are no longer necessary for legal purposes, and that no such data will be retained by CFCL or Mapped in for any other purpose. We therefore consider this aspect of the matter resolved.

Conclusion

[106] To conclude, we find that CFCL engaged in the collection and use of personal information through the deployment of the AVA technology in its shopping malls without ensuring knowledge, consent or notice.

[107] Consequently, we find that CFCL contravened: principles 4.3 of Schedule 1, as well as section 6.1, of PIPEDA; section 7(1) and section 13(1) of PIPA AB; and sections 6 and 10(1) of PIPA BC.

[108] Additionally, we determined that CFCL failed to ensure the timely disposal of personal information in the form of numerical representations of faces – and related information – collected through the deployment of the AVA technology in its shopping malls.

[109] Based on CFCL's commitments and facts outlined above, we accept that CFCL is currently in compliance with the Acts. We therefore consider this matter to be **well-founded and resolved**.

[110] That said, we wish to remind CFCL that regardless of whether it disagrees with our Office's findings, we expect that, should it implement AVA technology in its malls in future, it will do so in a manner that respects Canadian privacy laws, as reflected in our recommendations.

Issue 2: Whether CFCL's use of mobile device geolocation technologies resulted in the collection, use and/or disclosure of personal information, and if yes, whether CFCL obtained adequate consent for that collection, use and/or disclosure?

CFCL's Representations and our Investigation

[111] During our investigation, we asked CFCL how geolocation and MAC addresses were used, alone or in combination with other information, in order to determine whether CFCL had collected or used personal information in the context. In addition, we asked questions to determine whether CFCL obtained adequate consent for the collection and use of personal information, where required.

[112] In order to corroborate the information provided to us, and better understand the practices at issue, we also sought representations from Aislelabs, a third-party service provider under contract with CFCL.

Overview of CFCL's Geolocation Implementation

[113] CFCL established and maintains Wi-Fi networks at all of its retail properties in order to offer complimentary internet access to mall visitors.[39] When a visitor with a Wi-Fi enabled device enters one of CFCL's properties, their device will be detected by a wireless access point. During communication with the access point, information is collected from the visitor's device – including its geolocation, which can be defined as information allowing for the estimation of a physical location. In other words, CFCL utilizes Wi-Fi triangulation, using signals sent from visitors' devices, to calculate their approximate position. If the visitor chooses to connect to the Wi-Fi network, they must log in and provide additional information. CFCL contracted with a third party company, Aislelabs, to analyze the information collected via its Wi-Fi access points on its behalf.

[114] CFCL described two processes by which it collects information from Wi-Fi enabled devices: (i) "Anonymous Shopper Journey"; and (ii) "Logged In Shopper Journey".

i. "Anonymous Shopper Journey": When an individual with a Wi-Fi enabled device enters a CFCL property, their MAC address is detected, and used to create a randomized unique identifier as described at paragraphs 126 and 127. If the individual does not log in, then this unique identifier and associated geolocation information is the extent of the information collected.
ii. "Logged In Shopper Journey": If an individual chooses to log in to CFCL's Wi-Fi network with a mobile device, the device's MAC address is detected and

[39] As of February 14, 2019.

collected as described above, and the individual is **required** to agree to CFCL's Terms and Conditions and to provide additional personal information, such as full name and email address, in exchange for access.

Note: Subsequent to the issuance of our preliminary report, CFCL clarified, and Aislelabs verified, that when a user connects via this option, CFCL associates with the Wi-Fi account only the property at which the individual was present (e.g., CF Eaton Centre), not the individual's location within that property. Aislelabs explained that while its logged-in Wi-Fi service offers the option to associate geolocation information with the account, this functionality had not yet been activated in CFCL's "Logged In Shopper Journey" implementation.

[115] According to its submissions, CFCL employs geolocation technologies at all 19 of its retail properties in Canada,[40] these being:

Property	Province
CF Market Mall	Alberta
CF Chinook Centre	Alberta
CF Richmond Centre	British Columbia
CF Pacific Centre	British Columbia
CF Polo Park	Manitoba
CF Champlain	New Brunswick
CF Toronto Eaton Centre	Ontario
CF Sherway Gardens	Ontario
CF Lime Ridge	Ontario
CF Fairview Mall	Ontario
CF Markville Mall	Ontario
CF Shops at Don Mills	Ontario
CF Fairview Park	Ontario
CF Masonville Place	Ontario
CF Rideau Centre	Ontario
CF Galeries d'Anjou	Quebec
CF Carrefour Laval	Quebec
CF Promenades St-Bruno	Quebec
CF Fairview Pointe Claire	Quebec

[116] When we asked CFCL to explain the purposes for its deployment of the geolocation technologies, it represented that it is for "counting pedestrian traffic and obtaining rough user segmentation to support CF in managing pedestrian flow, and to establish the value of its properties to advertisers and merchants". In addition, CFCL uses what it

[40] As of February 14, 2019.

described as anonymous, aggregate information to research and develop new products and techniques to improve its services for consumers and retailers.

[117] CFCL stated that it did not employ geolocation "tracking" in its shopping malls, and instead indicated that the technologies it employs simply locate mobile devices to a general area or zone in its properties. CFCL took the view that it does not identify or track individuals, but mobile devices.

[118] Information provided by Aislelabs indicated that their indoor geolocation capabilities are based on a Wi-Fi positioning system that can triangulate the location of devices to an area referred to as a "zone". It represented that each CFCL property consists of multiple zones. For example, the Eaton Centre was described as having 29 zones. Each zone was characterized as having several retail outlets.

Further information regarding Analytics

[119] Aislelabs describes itself[41] as a technology company that offers Wi-Fi location marketing and advertising, as well as an analytics platform. For CFCL, it also builds audience profiles for visitors, complete with their behavior, interests and demographics based on information collected via the Logged In Shopper Journey.

[120] We note that although CFCL indicated that it does not store the information collected by Aislelabs on its behalf, the service agreement between the two parties stipulates that CFCL remains the owner of the information collected by the geolocation technologies:

> Aislelabs acknowledges that it obtains no ownership nor proprietary rights of any nature or kind in or to the Content or Your Data or any part thereof under the terms of this Agreement. All right, title and interest in and to the foregoing (including any and all related Intellectual Property Rights, modifications and additions) thereto shall at all times remain with You.

[121] Based on the terms of this contractual agreement, we understand that CFCL remains responsible for information collected by Aislelabs on CFCL's behalf.

[122] In their representations, Aislelabs confirmed that it does not use the information obtained in the context of their agreement with CFCL for any purposes other than to provide the contracted service. It was further stated that Aislelabs does not share any such information with third parties.

Anonymous Shopper Journey

[123] According to the information provided by CFCL, when a Wi-Fi-enabled mobile device enters one of its properties, the MAC address of the device is detected and collected, enabling Aislelabs' software to differentiate between first time and repeat visitors,

[41] Aislelabs, About Us.

calculate the approximate location of a device inside CFCL's properties via heat maps, and capture walking paths and "dwell time".

[124] Aislelabs, which collects and analyzes the information on behalf of CFCL, provides the latter with aggregated reports based on the collected information, which includes for example, statistics about the number of shoppers, repeat customers, time spent in a zone within a mall, top walking paths and heat maps representing shopper density within designated zones. CFCL is able to access those reports via a web-based dashboard.

[125] Both CFCL and Aislelabs represented that this process is "anonymous" because Aislelabs' software uses a technique called hashing, which consists of using a one-way function to assign a unique identifier to the mobile device in lieu of the actual MAC address. This process is completed before the identifier is saved onto Aislelabs' database. Hashing a unique identifier offers protection against reverse engineering (or other means aimed at recovering the original value) both by the organization collecting and holding the information and by third parties. While it is theoretically possible to reverse a securely hashed value, it is highly impractical. Our Technological Analysts confirmed that based on Aislelabs' representations, they are using an algorithm currently accepted as cryptographically secure.

[126] In addition to hashing the MAC addresses, Aislelabs represented that it further replaces each hashed MAC address with a random identifier, so that the hashed MAC addresses cannot be obtained from the value stored on its database. Therefore, outside of Aislelabs systems, the resulting random identifier cannot be linked to the original MAC address, providing an additional layer of depersonalization. This additional step further mitigates the risk of the original MAC address being recovered and associated to the geolocation data, by CFCL, Aislelabs or any unauthorized third party.

Logged In Shopper Journey

[127] The Logged In Shopper Journey also relies on the collection of MAC addresses, which are subsequently hashed, but CFCL advised that it collects additional personal information, with consent, when a mobile device is used to connect to its complimentary Wi-Fi service. Access to CFCL's Wi-Fi requires that the visitor sign up for an account. Accordingly, CFCL collects additional information via the account creation process, such as first and last name, email address, and language preference.

[128] CFCL represented that MAC addresses and geolocation information collected in the Anonymous Shopper Journey "are not, and cannot, be subsequently associated with the Logged In Shopper Journey". As such, at the time of account creation, no information is associated from previous visits made by the individual. Additionally, if a Wi-Fi user who has logged out of their account subsequently visits a CFCL property without signing in, MAC address and geolocation data will only be collected in the form of the Anonymous Shopper Journey. Information collected during the visit will only be associated to the

visitor’s account if they are logged in. CFCL further asserted that the information stored in the two solutions cannot be combined in any way.

[129] CFCL represented that it obtains express consent for this practice via the Terms & Conditions accessible from the login page, which incorporate the Privacy Policy explaining the practices in question.

[130] More specifically, according to CFCL, when a visitor wishes to use CFCL’s complimentary Wi-Fi service, they must log in using one of various available methods (i.e.: a social media account or email address), after agreeing to its Terms and Conditions (“T&C” or the “Terms”). The Terms shown on the Wi-Fi login contain the following:

> By accessing The Cadillac Fairview Corporation Limited’s Wireless Internet Service you agree to comply with the Terms of Service. If you do not accept the Terms, do not access or use the Service. The following summary of the Terms is provided for your convenience. Please read the full Terms of Service below.
>
> Summary
> 1. You will act lawfully, responsibly and reasonably while using the Service.
>
> 2. You assume full responsibility for your use of third party websites while using the Service.
>
> 3. Under no circumstances will Cadillac Fairview be liable as a result of your use or inability to use the Service.
>
> 4. You agree to indemnify and hold harmless Cadillac Fairview from any all claims, relating to or arising out of your use of the Service.
>
> 5. There is no guarantee of the privacy or security of any transmission made or received through the Service.
>
> 6. As a complimentary Service, it is provided without any warranties. Cadillac Fairview does not warrant the availability or reliability of the Service.
>
> 7. Cadillac Fairview reserves the right to block certain internet websites or services, and may revoke your access to the Service at any time.
>
> 8. Cadillac Fairview may monitor your activity in connection to the Service and may disclose any information related to, as necessary.
>
> **9. Personal information will be used as set forth in our Privacy Policy** [emphasis added]
>
> 10. The Service and the Terms may change without notice. You should check back to see the Terms in effect. Your continued use of the Service will constitute your acceptance of the Terms.
>
> Click **here** to accept and continue to the Wi-Fi.
>
> Click **here** to read the full Terms and Conditions.

[131] As highlighted in the above excerpt, the summary says that “Personal information will be used as set forth in our Privacy Policy”, with an embedded link. We note that this link

is actually not a link to CFCL's Privacy Policy, but instead takes individuals to a page titled "CF SHOP! Privacy Statement". Individuals must scroll to the bottom of the page to view the link to CFCL's actual Privacy Policy.

[132] CFCL asserted that when an individual accepts the Wi-Fi Terms, the device user provides their consent to CFCL's collection and use of their personal information, and that since "Wi-Fi Terms and Conditions expressly reference the Privacy Policy, [they] incorporate it". Should individuals choose not to accept the Terms, they would be denied use of the complimentary Wi-Fi service. While the summary does highlight provisions relating to limiting CFCL's liability, and appropriate use of the Wi-Fi service, there is no specific mention of privacy practices, beyond a link to the CF SHOP! Privacy Statement.

[133] In the full T&C document, CFCL informs users of the Wi-Fi Service (the "Service") that it may monitor, log and review users' activities in connection with their use of the Service. Further, it states that "[a]ny personal information you supply to us for the purposes of accessing the Service will be used as set forth in our Privacy Policy, which can be found at http://cfshop.ca/privacy.html and these Terms".

[134] Specifically, CFCL pointed to certain sections of the Privacy Policy, including, under the section "Browser and Device Information"

> We may also use device information such as MAC address or other device identifiers to track foot-traffic, deliver relevant promotions and offers, customize your online experience, and to provide and manage our WIFI services.

Another section asks "Do you use cookies, ibeacons and other similar technologies?" and says:

> We also use a variety of technologies to track foot traffic and mobile devices within our properties. This technology allows us to gather information on how our properties are used and also allows us (with your permission) to provide you with special location-based offers.

[135] We also noted the following, under the section "What types of personal information do you collect and use?":

> Location Information … We use location-based information to understand how our premises are used, and to provide you with location-based offers.

Under the heading "Do you customize promotional offers and other benefits for me?", the policy states:

> Please see 'What choices do I have?' for information on opting-out of these personalized promotional offers and other benefits.

and under "What choices do I have?", the Privacy Policy says:

> Location Information. We only collect your location information in a manner that is associated with you if you are logged into our mobile applications and authorize your device to provide us with GPS information.

Opt-Out Option

[136] Aislelabs explained to our Offices that individuals have the choice to opt out of having an identifier associated to location-based analytics conducted by Aislelabs on behalf of its clients, like CFCL, by entering the MAC address of their mobile devices at an opt-out webpage.[42] Once an individual enters the MAC address of their device, information that may have previously been associated with that device is discarded.

[137] We found no reference to, or explanation of, this opt-out option in CFCL's Privacy Policy.

Analysis

Was there Collection, Use and/or Disclosure of Personal Information?

[138] First, we considered whether the information collected by CFCL using the geolocation technologies constituted personal information as defined in subsection 2(1) of PIPEDA, section 1 of PIPA BC and section 1(1)(k) of PIPA AB. The Acts define personal information as information about an identifiable individual.

Anonymous Shopper Journey

[139] For the reasons outlined below, we accept that CFCL is not collecting personal information in the context of the "Anonymous Shopper Journey".

[140] Contrary to CFCL's position that MAC addresses are "simply not personal information", we are of the view that a MAC address can constitute personal information, whether it be in its original form or hashed, in certain circumstances. In our view, however, they do not constitute personal information in the circumstances of the Anonymous Shopper Journey.

[141] Courts have found in various cases that personal information must be given a broad interpretation as to give effect to the legislation's intended purpose.[43] Additionally, personal information will be considered as such if it is "about" identifiable individuals, and individuals will be considered as being identifiable when the information in question, disclosed alone or together with other publicly available information, "would

[42] This option is made available via a website, which allows for individuals to enter their MAC address in order to opt out of Aislelabs' Mobile Location Analytics, and that of other companies. The website is described as a project owned by the Future of Privacy Forum, a non-profit organization self-described as "advancing principled data practices in support of emerging technologies".

[43] *Dagg v. Canada* (Minister of Finance), [1997] 2 S.C.R. 403, dissenting, at para 68; Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board), 2006 FCA 157.

tend to or possibly identify them."[44] Moreover, "about" is also defined as being information that is not just the subject of something but also relates to or concerns the subject.[45]

[142] We note CFCL's submissions in relation to the *Leon's*[46] case, which held that information must be identifiable and personal (i.e., directly related to the individual) in order to constitute personal information. That said, the Federal Court has more recently cautioned that information about devices and objects could still be considered personal information if it can be associated with an identifiable individual in a manner or context that reveals personal information.[47] Furthermore, subsequent to *Leon's*, a decision[48] made by the Alberta Court of Appeal states that "[w]here the information related to property, but also had a "personal dimension", it might sometimes properly be characterized as "personal information".

[143] Information that is not, on its face, personal information, can still be considered as such if "there is a serious possibility" that an individual could be identified through the use of that information, alone or in combination with other available information.[49] The application of this threshold depends on the circumstances of each case. For there to be a "serious possibility", it must be beyond mere speculation, but does not need to reach the level of "more likely than not".[50]

[144] The OPC has expressed its view in a number of previous cases that device identifiers can constitute personal information, and be about an identifiable individual. For example, in a 2013 investigation into WhatsApp,[51] the OPC found that unique identifiers, user's device identifier information, mobile subscriber ID, mobile country code, and mobile network code could constitute personal information, since the information, alone or in combination with other information, could render a specific individual identifiable. The OIPC BC has also issued investigation reports that cite device identifiers as a form of personal information. For example, a 2019 report on medical clinics found that clinics should be notifying individuals before collecting personal information online, including

[44] *Girao v. Zarek Taylor Grossman Hanrahan LLP*, 2011 FC 1070 para 32.

[45] *Canada (Information Commissioner) v. Canada (Transportation Accident Investigation and Safety Board)*, 2006 FCA 157 (CanLII)

[46] 2011 ABCA 94 [*Leon's*].

[47] *Canada (Information Commissioner) v. Canada (Minister of Public Safety and Emergency Preparedness)*, 2019 FC 1279.

[48] *Edmonton (City), v. Alberta (Information and Privacy Commissioner)*, 2016 ABCA 110 at para 25, upholding in part 2015 ABQB 246

[49] *Ibid* at para 34.

[50] *Ibid* at para 53.

[51] *See e.g.,* Investigation into the personal information handling practices of WhatsApp Inc; Apple called upon to provide greater clarity on its use and disclosure of unique device identifiers for targeted advertising; Employee text messages intercepted without authorization at the Warkworth Institution.

device identifiers, and recommended that device identifiers and other personal information collected, used, or disclosed online should be detailed in privacy policies.[52]

[145] A MAC address, depending on the context, can be personal information, for example when combined with other available information. In the case of the Anonymous Shopper Journey, the only information associated with the hashed MAC address is general and imprecise geolocation information limited to CFCL malls and their immediate surroundings. This information is not, in our view, sufficient to allow an individual to be identified as it does not contain the geographic scope or level of detail required to extrapolate identifying information such as residence, routine or specific place of employment. Furthermore, the hashing and randomization of the MAC address would render it practically infeasible to use the MAC address to link other available information about the mobile device user, such that we accept that there is not a serious possibility that the MAC address, or associated geolocation information, could be linked to that user.

[146] We therefore accept that CFCL is not collecting, using or disclosing personal information in the specific context of the Anonymous Shopper Journey, as understood by this investigation.

Logged In Shopper Journey

[147] As noted above, CFCL acknowledged that for its Logged In Shopper Journey, it does collect personal information via login, such as email addresses and other personal information that is provided depending on the login mechanism. In particular, CFCL represented that when visitors opt to sign into Wi-Fi using a social media account, it will collect other information associated with the account. This information is then associated to the Logged In Shopper Journey Account. It is our view that the MAC addresses and any geolocation information collected while the user is logged in would become personal information due to their association with a user account, and thus an identifiable individual.

[148] Based on the new information provided to our Offices by CFCL and Aislelabs in response to our preliminary report, we now understand and accept that CFCL does not, and cannot practically, associate geolocation information derived via Wi-Fi triangulation, the subject of our investigation, with the personal information of logged-in shoppers. While theoretically, there exist methods by which CFCL could, via Aislelabs, make such an association, MAC address hashing and database separation render linking impractical.

[149] Contractual and code restrictions exist. While Aislelabs may have the technical capability to link geolocation data on CFCL's WiFi network, the company would be precluded from doing so pursuant to both their contract with CFCL and the Mobile Location Analytics

[52] *See e.g.,* OIPC BC. Audit & Compliance Report P19-01: Compliance Review of Medical Clinics.

Code of Conduct to which they have confirmed their strict adherence. We have no evidence that Aislelabs ever attempted to make such a link, and in our view, the information in question – an approximate location of visitors within the confines of malls – would not be of justifiable value to breach contractual obligations and codes of conduct.

[150] Our Offices have not considered whether CFCL obtained valid consent for information obtained from third-party social media accounts via log-in through the single sign-on process, which is outside the scope of this investigation.

Was there Valid Consent and Notice for collection of MAC Address and geolocation information?

[151] Given our conclusion that CFCL is not collecting personal information via its Anonymous Shopper Journey, we accept that it did not require consent to collect that information.

[152] With respect to the Logged In shopper Journey, when we issued our preliminary report, we understood that CFCL was associating geolocation information derived via Wi-Fi triangulation to the accounts of individuals using CFCL Wi-Fi. As such, we conducted a preliminary analysis with respect to the adequacy of CFCL's consent for that practice. We have now learned via CFCL's response to our preliminary report, that it was <u>not</u> associating, or linking, such geolocation information about individuals using the Wi-Fi service.[53] While CFCL was, concurrent with the Logged In Shopper Journey, collecting triangulated location information about Wi-Fi enabled devices via the Anonymous Shopper Journey, we determined that this was not personal information in that context. Furthermore, CFCL was not associating, and could not practically associate or link that information to personal information collected about Wi-Fi users.

[153] We note, however, that Aislelabs' logged-in Wi-Fi service offers the <u>option</u> to associate triangulated "zone" information to accounts, and that CFCL did include, in its privacy policy, the assertion of using geolocation information to deliver location-based offers (see paragraph 135). We have, therefore, included our analysis with respect to the association of geolocation data with Wi-Fi accounts below, to explain our Offices' expectations should CFCL decide to activate this functionality in the future.

Meaningfulness

[154] Principle 4.3 of Schedule 1 of PIPEDA states that the knowledge and consent of the individual are required for the collection, use, or disclosure of personal information.

[53] While CFCL does collect very limited "location" information for logged-in users – i.e., the mall at which the individual has logged in to the Wi-Fi - this is not Wi-Fi-triangulated geolocation information, and is outside the scope of our investigation. That said, we note that as per paragraph 170, CFCL has now added language in its privacy statement to clarify that only the name of the CFCL property at which individuals connect, and <u>not</u> more granular location information, is associated with Wi-Fi accounts.

Principle 4.3.2 of PIPEDA further provides that an organization must make a reasonable effort to ensure that the individual is advised of the purposes for which the information will be used and that to make the consent meaningful, the purposes must be stated in such a manner that the individual can reasonably understand how the information will be used or disclosed. Section 6.1 of PIPEDA further clarifies that for consent to be valid, it must be reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose and consequences of the collection, use, or disclosure of the personal information to which they are consenting.

[155] Similarly, section 7(1)(a) of PIPA AB states that, except where otherwise authorized in the Act, "[…] an organization shall not, with respect to personal information about an individual […] collect that information unless the individual consents to the collection of that information". Section 13(1) of PIPA AB further requires that before or at the time of collecting the individual's personal information from the individual, the organization must notify the individual in writing or orally of the purposes for which the information is collected. The notice must also include the name, position, or title of a person who is able to answer on behalf of the organization the individual's questions about the collection.

[156] In the same vein, subsection 7(1) of PIPA BC states that an individual has not consented unless they have been given notice. In some cases, notice is not required if the purpose for the collection, use or disclosure is "obvious" and the individual volunteers their information for that purpose. Section 10(1) of PIPA BC further provides that on or before collecting personal information about an individual from the individual, an organization must disclose to the individual verbally or in writing the purposes for the collection of the information. The organization must, upon request, also provide the position name or title and the contact information for an officer or employee of the organization who is able to answer the individual's questions about the collection.

[157] Further to the above, the Guidelines provide that individuals should be made aware of **all** purposes for which information is collected, used or disclosed. These purposes must be described in meaningful language, avoiding vagueness like 'service improvement', and should not be buried in a privacy policy or terms of use as it serves no practical purpose to individuals with limited time and energy to devote to reviewing privacy information.

[158] The Guidelines also provide that "to receive meaningful consent, organizations must allow individuals to quickly review key elements impacting their privacy decisions right up front as they are considering using the service or product on offer…" and that "organizations should in particular highlight any purposes that would not be obvious to the individual and/or reasonably expected based on the context" [emphasis added].

[159] We note that the summary of the Terms & Conditions for accessing CFCL's Wi-Fi service includes 10 specific points, only one of which relates to privacy, and then only to the extent of saying "Personal information will be used as set forth in our Privacy Policy".

The summary does not speak, even at a high level, about what personal information will be collected, nor the purpose(s) for which that information will be used. To find this information, individuals must click the hyperlink to access a Privacy Statement, and then find the link to CFCL's Privacy Policy at the bottom of that page. Many users will not, before logging in, or ever, read that 5,000 word document.

[160] Consent is only valid or meaningful where individuals understand what they are consenting to. As such, in our view, should CFCL decide, in future, to collect and use triangulated or more precise geolocation information of Wi-Fi users (for example to deliver location based offers as previously stated in their Privacy Policy), CFCL would need to ensure that prospective users are made aware of this practice via a prominent notice on the log-in page before they "Click here to accept and continue to the Wi-Fi", and a clear and detailed explanation of the practice in its Privacy Policy.

[161] Finally, we note that CFCL does not currently use geolocation information to deliver "special location-based offers", contrary to what it stated in its Privacy Policy. In our view, CFCL cannot meaningfully explain the manner in which it would use or disclose personal information to achieve these purposes, when it does not in fact engage in such a practice. As such, in our view, it should not be seeking such consent at this time.

Choice

[162] The Acts provide that individuals shall not be required to consent to the collection, use or disclosure of personal information beyond what is necessary to provide a product or service.[54]

[163] The Guidelines further explain that for a collection, use, or disclosure to be a valid condition of service, it must be integral to the provision of that product or service and that where it is not, individuals must be given a choice. Purposes integral to the provision of the service should be distinguished from those that are not, and any available options must be explained clearly and made easily accessible.

[164] CFCL advertises complimentary Wi-Fi as a service to entice potential shoppers to spend time at its malls. In our view, CFCL benefits from the provision of this service through

[54] Principle 4.3.3 of PIPEDA stipulates that an organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.

Section 7(2) of PIPA AB states that an organization shall not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information about an individual beyond what is necessary to provide the product or service.

Section 7(2) of PIPA BC provides that an organization must not, as a condition of supplying a product or service, require an individual to consent to the collection, use or disclosure of personal information beyond what is necessary to provide the product or service.

the potential for increased mall traffic, even without the collection of geolocation data. While we recognize the legitimate business benefits that CFCL could potentially gain from the collection, use and disclosure of personal information via geolocation technologies and related analytics, geolocation tracking would not be integral to providing Wi-Fi services. As such, CFCL should provide individuals with the ability to opt-out should it decide to collect and associate triangulated, or more precise geolocation data with logged-in Wi-Fi accounts in the future.

Preliminary Recommendations

[165] In our preliminary report, we recommended that CFCL take the following measures to ensure meaningful consent for its use of MAC address and geolocation information of individuals accessing its logged in Wi-Fi service:

i. provide clear and prominent language, for example on the Wi-Fi log-in page, highlighting its geolocation tracking practices, the purposes for which it will use that information and how users can opt-out of the practice;

ii. provide individuals with an easily accessible and conspicuous opt-out option for CFCL's association of their MAC address and geolocation information to accounts;

iii. include in its privacy policy a clear explanation that geolocation tracking is not integral to the provision of its Wi-Fi service, and explaining how individuals can opt out of the practice; and

iv. cease seeking consent for the use of geolocation and MAC address for purposes of delivering "special location-based offers" until such time as CFCL plans to engage in that practice, and is therefore able to meaningfully explain how it will use that information for such purposes.

CFCL's Response to our Recommendations

[166] As outlined above, in response to our preliminary report, CFCL provided new information to our Offices confirming that it did not associate zone-based geolocation information to individual Wi-Fi accounts.

[167] We note, however, the potential for zone-based geolocation information to be associated to the Logged In Shopper Journey using Aislelabs service (functionality that was not included in CFCL's current Wi-Fi implementation), and the fact that CFCL's Privacy Policy had asserted the use of geolocation information to provide "special location-based offers".

[168] We therefore asked that CFCL commit to follow the recommendations set out in paragraph 165 (i through iii) should it decide to activate the association of geolocation data with logged in Wi-Fi accounts in the future.

[169] CFCL refused to make this commitment, asserting that our recommendations were speculative.

[170] CFCL did, however, commit to cease seeking consent for the use of geolocation and MAC address for purposes of delivering “special location-based offers”, a practice in which it did not engage, and to clarify that only the name of the CFCL property at which individuals connect, and not more granular location information, is associated with Wi-Fi accounts. In response to our preliminary report, CFCL has amended the language in its Privacy Policy accordingly.

Conclusion

[171] On the issue of consent for collection, use and disclosure of geolocation, we find that CFCL did not collect personal information in the context of the Anonymous Shopper Journey, and did not collect triangulated geolocation information in the context of the Logged In Shopper Journey. We therefore conclude that the matter is **not well-founded.**

[172] That said, we wish to remind CFCL of our expectation that should it associate zone-based or more granular geolocation information to Wi-Fi accounts in its malls in the future, it would do so in a manner that complies with Canadian privacy laws, as reflected in our preliminary recommendations.