Information and Privacy Commissioner,
Ontario, Canada

Commissaire à l'information et à la protection de la vie privée,
Ontario, Canada

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT PX24-00001

University of Waterloo

June 11, 2025

Summary: The Office of the Information and Privacy Commissioner of Ontario (IPC) received complaints from students at the University of Waterloo (the university) regarding "smart" snack vending machines installed on campus by a third-party service provider. The complaints alleged that the machines appeared to use facial recognition technology that was collecting facial images without consent or proper notice.

In this report, I find that the machines used cameras and face detection technology to capture identifiable facial images amounting to a collection of personal information within the meaning of section 38(1) of the *Freedom of Information and Protection of Privacy Act* (*FIPPA*). Further, I find that this collection did not comply with section 38(2) of *FIPPA* and, therefore, was a privacy breach. I also find that affected individuals were not given notice of the collection, as required under section 39(2) of *FIPPA*.

Although the university had reasonable contractual safeguards in place with the third-party service provider, it was unaware that personal information was being collected through the machines' face detection technology. This oversight was due to shortcomings in the university's procurement process for the vending machines which failed to apply the necessary level of due diligence by conducting a privacy impact assessment, or requiring prospective service providers to do so, in order to identify and assess the privacy implications of the technology.

In this report, I recommend that the university take adequate steps in the procurement process to ensure it evaluates third-party service providers and any technology to be used, and fulfills its obligations to protect personal information under its control in accordance with section 4(1) of Regulation 460 under *FIPPA*.

Statutes Considered: The *Freedom of Information and Protection of Privacy Act,* R.S.O. 1990, c. F. 31, (*FIPPA*) sections 2(1), 38(1) and (2), and 39(2); and Regulation 460 under *FIPPA,* section 4(1); The University of Waterloo Act, 1972*,* SO 1972, c 200, ss. 2, 4, 14.1(c), (f) Legislation Act, 2006, S.O. 2006, c. 21, Sched. F**,** s. 92(1).

Orders and Investigation Reports Considered: Order PO-1880, Order 11, Privacy Complaint Reports PI21-00001, PR16-40, MC10-2, MC07-68; Privacy Investigation Report PC12-39; Joint Investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia.

Cases Considered: *Cash Converters Canada Inc. v Oshawa (City)*, 2007 ONCA 502, 86 OR (3d) 401; *Reference re Assisted Human Reproduction Act*, 2010 SCC 61; *Reference re Genetic Non-Discrimination Act*, 2020 SCC 17; *Reference re Securities* Act, 2011 SCC 66, [2011] 3 SCR 837; *Ontario Criminal Code Review Board v. Hale*, 47 O.R. (3d) 201 (C.A.).

Secondary Sources: Mahmud Jamal, "Is PIPEDA Constitutional", 43 Can. Bus. L.J. 434 (2006), at pp. 442, 448; Michel Bastarache, "The Constitutionality of PIPEDA: A Reconsideration in the Wake of the Supreme Court of Canada's *Reference re Securities Act*", June 2012, at pp. 4-6, 11-12; Josh Nisker, "PIPEDA: A Constitutional Analysis, Canadian Bar Review, Vol. 85, p. 317 (2006), at pp. 326-329.

BACKGROUND:

[1] In February 2024, news media reported that University of Waterloo (the university) students had raised privacy concerns about smart snack vending machines installed on their main campus, after one of the machines malfunctioned and displayed the following software error message:

> Invenda.Vending.FacialRecognition.App.exe – Application Error[1]

[2] Additionally, it was reported that the machines were supplied by Adaria Vending Services Limited (Adaria), owned by MARS Wrigley (MARS) and manufactured by Invenda Group (Invenda).[2]

[3] The Office of the Information and Privacy Commissioner of Ontario (IPC) received complaints from the university's students about the machines. The students believed that the machines had captured images of their faces and complained that they were not informed of the apparent use of facial analytics technology. They also complained that they had not consented to the collection of their facial images, which they consider to be

[1] https://www.theguardian.com/world/2024/feb/23/vending-machine-facial-recognition-canada-univeristy-waterloo, https://mobilesyrup.com/2024/02/27/university-of-waterloo-vending-machine-facial-recognition/ and 'Facial recognition' error message on vending machine sparks concern at University of Waterloo | CTV News.

[2] See footnote 1.

personal information.

[4] As such, the students believed that the university had breached their privacy under the *Freedom of Information and Protection of Privacy Act* (*FIPPA*). As a remedial measure, they requested that the machines be removed from campus.

[5] An investigation was commenced into this matter, and written representations and relevant materials were requested and received from the university.

The University, Adaria, MARS, Invenda and the Vending Machines

[6] The machines at issue are intelligent vending machines (IVMs) manufactured by Invenda, a software company that makes automated retail devices smart and connects them to a single digital platform.[3]

[7] In response to this office's request for information about the matter, the university advised that, in October 2023, it entered into an agreement with Adaria to provide 29 unattended snack vending services on its main campus (the Agreement). Under this agreement, Adaria was responsible for maintaining, monitoring and stocking the IVMs, which it installed on the university's campus in December 2023.

[8] According to the university, Adaria either purchased or leased the machines from MARS and MARS contracted with Invenda to manufacture and supply the IVMs that were installed on the campus. The university also advised that it did not contract with MARS or Invenda and was informed there was no contract between Adaria and Invenda concerning the IVMs.

[9] Regarding the technology used in the IVMs, the university explained that the machines were equipped with a computer running a customized installation of the Windows operating system that Invenda calls "Invenda OS", which collected data from the IVMs and transmitted it over the Internet to a cloud service operated by Invenda, known as the Invenda Platform.

[10] The university further advised that, without its knowledge, the IVMs used face detection technology that collected demographic data.

The University's Jurisdictional Challenges

[11] Throughout this investigation, the university raised several grounds challenging the IPC's jurisdiction to investigate the potential collection of personal information through the operation of the IVMs on its campus, as well as the scope of any such investigation. While the university ultimately responded to our requests for information, its cooperation with the investigation came with the following caveat:

[3] https://www.invendagroup.com/our-story and https://www.invendagroup.com/vending-machines.

> The University continues to question the jurisdiction of the Commissioner to carry out an investigation into an alleged breach of personal information through vending machines on its campus but intends to cooperate with the Commissioner so that this matter can be resolved.

[12] First, the university took the position that *Personal Information Protection and Electronic Documents Act* (*PIPEDA*), and not *FIPPA*, applied to the operation of its commercial activities based on the federal power of Parliament over "the regulation of trade and commerce." In support of this position, the university cited a publication by the Office of the Privacy Commissioner of Canada (OPC) concerning the application of the *PIPEDA* to Municipalities, Universities, Schools, and Hospitals.[4] In the university's view, the sale of food items through the vending machines constituted a commercial activity unrelated to its core purpose of providing post-secondary education, with the result that *PIPEDA* would govern any collection of personal information by the vending machines to the exclusion of *FIPPA*.

[13] Second, the university cited Invenda's assertion that the IVMs did not, in fact, collect any personal information. It argued that, if no personal information has been collected, then the IPC cannot have jurisdiction to conduct an investigation under *FIPPA*.

[14] Third, while the university accepted that it is accountable for the collection, use or disclosure of personal information by third party service providers, and is responsible for their management, it maintained that it did not contract with Adaria to collect personal information using face detection technology. Because any collection of personal information by the IVMs fell outside the scope of the contracted services, the university argued that Adaria was not its service provider in this context. On this basis, the university submitted that any investigation into the matter by the IPC should be limited to their vendor due diligence and management practices.

[15] Finally, the university maintained there was no need for the IPC to investigate the matter because the face detection technology in the IVMs was disabled in February 2024, the machines were removed from campus in March 2024, with no plans to reinstall them, and all data that was collected has since been permanently deleted.

[16] Turning to the constitutional argument, the university appears to take the position that Parliament's power over federal trade and commerce under section 91(2) of the *Constitution Act, 1867* means that *PIPEDA's* regulation of personal information in the context of the university's commercial operates to the exclusion of *FIPPA*.

[17] The university's position is not supported by the provisions of *FIPPA* establishing its scope and application. Nor is this position supported by any judicial authority.

[18] The views expressed in the OPC's publication with respect to the "core" activities

[4] The Application of PIPEDA to Municipalities, Universities, Schools, and Hospitals - Office of the Privacy Commissioner of Canada.

of provincial and municipal institutions are not reflected in the provisions of *FIPPA*. Notwithstanding the potential application of *PIPEDA* to the commercial activities of third-party vendors, the university retains control over personal information of its students collected by commercial vendors operating on its behalf and under its authority. This gives rise to commensurate responsibilities to ensure by contractual or other means that vendors' activities in the handling of such personal information comply with the provisions of *FIPPA*.[5] Whether or not the collection of personal information has a commercial purpose or component has no bearing on the university's obligations to protect the personal information under its control in accordance with *FIPPA*.[6]

[19] There is a broad consensus among the judiciary and legal commentators that the relationship between organizations and individuals in the handling of their personal information falls within the "property and civil rights" head of power at section 92(13) of the *Constitution Act, 1867* or "generally all matters of a merely local or private nature in the province" at section 92(16).[7] Nonetheless, the constitutional division of powers jurisprudence recognizes that a particular subject matter can have both federal and provincial aspects, in which case the "double aspect doctrine" allows for the concurrent application of both federal and provincial legislation.[8]

[20] In a 2006 article supporting the constitutional validity of *PIPEDA* under the federal trade and commerce power, Mahmud Jamal (now Justice of the Supreme Court), stated that "the protection of personal information arguably has a double aspect" and, as such, "both levels of government may legislate in one jurisdictional field for two different purposes." He further opined that "the protection of personal information is arguably not a single matter" but "cuts across both federal and provincial fields and is not assigned exclusively to either level of authority".[9]

[21] To the extent that minimum national privacy standards are seen as necessary to promote Canadian economic interests, legal scholars have concluded that *PIPEDA* may be viewed as constitutionally valid under the trade and commerce power at section 91(2) pursuant to the "double aspect doctrine".[10] That is the conclusion reached in a 2022 legal opinion commissioned by the OPC examining the constitutional validity of proposed

[5] I note that the agreement the university entered into with Adaria provided that the university owned all personal information "submitted to or created by" Adaria, who agreed to handle it in compliance with all applicable privacy laws.

[6] An example of an IPC Privacy Investigation Report relating to an institution's commercial activities is found in Privacy Complaint PR16-40; Ontario Lottery and Gaming Corp. (Re), [2019] O.I.P.C. No. 11 (QL).

[7] *Reference re Assisted Human Reproduction Act*, 2010 SCC 61; *Reference re Genetic Non-Discrimination Act*, 2020 SCC 17; Mahmud Jamal, "Is PIPEDA Constitutional", 43 Can. Bus. L.J. 434 (2006), at pp. 442, 448; Michel Bastarache, "The Constitutionality of PIPEDA: A Reconsideration in the Wake of the Supreme Court of Canada's *Reference re Securities Act*", June 2012, at pp. 4-6, 11-12; Josh Nisker, "PIPEDA: A Constitutional Analysis, Canadian Bar Review, Vol. 85, p. 317 (2006), at pp. 326-329.

[8] *Reference re Securities Act*, 2011 SCC 66, [2011] 3 SCR 837, para. 66.

[9] Mahmud Jamal, "Is PIPEDA Constitutional", 43 Can. Bus. L.J. 434 (2006) at pp. 442, 448.

[10] The constitutional validity of *PIPEDA* has not been tested in the courts. Jamal, at pp. 448-449; Nisker, at pp. 326, 329, 343.

successor legislation to *PIPEDA*, entitled "The Constitutional Validity of Bill C-11, the *Digital Charter Implementation Act*" ("OPC Opinion"),[11] where the authors state:

> … [T]he regulation of privacy can exist under both federal and provincial jurisdiction. Parliament is entitled to protect privacy in so far as it impacts national economic interests — jurisdictional silos are not required. Parliament's jurisdiction to promote the economy through the protection of privacy *does not strip provincial ability to further protect privacy* (emphasis added). [12]

[22] The OPC opinion underscores the conclusion that *PIPEDA* cannot override the privacy provisions of *FIPPA* or oust the oversight and reporting functions of the Commissioner under *FIPPA* in relation to the activities of the University at issue here, including its intra-provincial commercial activities.

[23] Accordingly, and notwithstanding the potential application of *PIPEDA*, it is clear that *FIPPA* also applies to any personal information collected by or on behalf of the university, including in the course of its commercial activities.

[24] The remainder of the university's so-called jurisdictional challenges actually comprise the substantive issues to be examined in this investigation report. Despite Invenda's assertion that no personal information was collected by the IVMs, that issue remains to be determined and will be examined below. The university's position that it did not contract with Adaria to collect personal information using face detection technology, and in fact was unaware of the use of this technology, raises questions about whether adequate privacy protections were, or should have been, in place with respect to the university's procurement and tendering processes.

[25] While it is acknowledged that the IVM's have been removed from campus grounds, the circumstances of this investigation require assurance that any personal information collected by the IVMs along with any derivative information has in fact been deleted or destroyed and will not be collected again in this way in the future.

[26] All of this is in aid of the IPC fulfilling its mandate under section 58 of *FIPPA* to report annually to the Legislative Assembly on the effectiveness of *FIPPA* in protecting personal privacy, including an assessment of the extent to which institutions are complying with *FIPPA* and the IPC's recommendations with respect to the practices of particular institutions.[13]

[11] At that time Bill C-27 had received second reading.

[12] Addario Law Group, LLP, The Constitutional Validity of Bill C-11, the *Digital Charter Implementation Act*, March 32, 2022, PDF, p. 11.

[13] Section 58 of *FIPPA*.

ISSUES:

A. Did the university's use of face detection technology result in a collection of personal information on the university's behalf under *FIPPA*?

B. Did the collection of personal information comply with sections 38 and 39 of *FIPPA?*

C. Did the university have reasonable measures in place to protect personal information in accordance with section 4(1) of Regulation 460 under *FIPPA*?

DISCUSSION:

A. Did the university's use of face detection technology result in a collection of personal information on the university's behalf under *FIPPA*?

[27] Section 2(1) of *FIPPA* defines "personal information" as "recorded information about an identifiable individual." Recorded information is information recorded in any format, including by electronic means or otherwise.[14]

[28] Information is "about" an individual when it refers to them in their personal capacity, which means that it reveals something of a personal nature about them. Information is about an "identifiable individual" if it is reasonable to expect that the individual can be identified from the information, either by itself or if combined with other information.[15]

[29] Section 2(1) lists examples of personal information. The list is not exhaustive, meaning that other kinds of information may also be personal information.[16]

[30] In this matter, images of individuals' faces were captured by the IVMs and data relating to these images, including estimates of their gender and age,[17] was generated. Accordingly, I must determine whether these images and any resulting data qualify as "personal information" as defined in section 2(1).

The Face Detection Technology

[31] The university advised that the IVMs were equipped with a (low-resolution) optical sensor that continuously captured visual input. According to the university, the sensor's resolution was too low to be considered a camera or create an identifiable image.

[14] See the definition of "record" under section 2(1) of *FIPPA*.
[15] Order PO-1880, upheld on judicial review in *Ontario (Attorney General) v. Pascoe*, [2002] O.J. No. 4300 (C.A.); 2001 CanLII 26053 (ON IPC).
[16] Order 11, [1988] O.I.P.C. No. 11**.**
[17] See Invenda's brochure regarding IVM at https://a.storyblok.com/f/184550/x/e94dbdaff3/product-catalogue-ovm-ivm_2024.pdf?cv=1714124864949.

[32] The university advised that one of the processes detected and counted moving objects while adding a timestamp. The university explained that the face detection software assumed these objects were people walking by the IVM and that these events were recorded and uploaded to the Invenda Platform.

[33] The university advised that the other process attempted to detect faces by analyzing the recorded image of the object (i.e. a person's face) that was close to the IVM. Using open-source libraries, the technology would estimate the gender (i.e. male, female or unknown) and age range of the person (together, the demographic data).

[34] When a sale occurred, the university advised that the IVMs would record a timestamp, the item purchased and the demographic data. The university also advised that the IVMs collected heatmap data to track where users touched the interactive display. It would then upload all this data to the Invenda Platform.

[35] According to the university, the technology could only estimate the demographic data at most 80% of the time, with 20% or more of the transactions recorded as "unknown" for this data, and that the accuracy confidence level was 60-80%.

[36] The university submitted that the face detection software in the IVMs processed facial images in a way that respected individual privacy. More specifically, the university asserted that the software:

- performed face detection, not face recognition and, therefore, did not identify or track individuals;
- processed recorded facial images in real time and, therefore, at no point was this data permanently stored or transmitted elsewhere; and
- converted recorded facial images into abstract and anonymous numeric descriptors representing an aggregate of the demographic data that could not be linked to any specific individual.

[37] The face detection software at issue was a third-party audience measurement (stand-alone) application[18] called VidiReports developed by Quividi.[19]

[38] The university stated that VidiReports was installed by Invenda, and that the "FacialRecognition.App.exe" application referenced on the malfunctioning IVM's display screen is an Invenda component, responsible for receiving data from third-party audience measurement services to create metadata stored for statistical purposes.

[18] The university advised that Invenda did not customize VidiReports for use within the IVMs.

[19] The Quividi and Data Security document states that "Quividi is a European company whose product line includes software solutions used to detect and qualify the presence of people in front of an object of interest and, in particular, in front of screens in a Digital Signage installation". For more information about Quividi visit: https://quividi.com/.

[39] The university provided this office with the following documents related to VidiReports and the demographic data:

- Quividi – FAQ;
- Quividi and Data Security;
- Quividi and Privacy Protection;
- Quividi's VidiReports and Biometry;
- (Quividi) Body Detection in VidiReports (together, the Quividi Materials); and
- (Invenda) Demographic Detection Data Schema.

[40] According to the Quividi Materials, their "solutions don't rely on biometric data to produce metrics", rather, they "are designed to detect and classify a face, or person, 'at large', using very generic patterns"[20] and, therefore, Quividi asserts that VidiReports relies on face detection, not face recognition.[21]

[41] Further, the Quividi Materials state that when VidiReports processes facial images:

- no data unique to an individual is ever generated;
- no biometric information is ever extracted; and
- no recognition or (re)identification is possible.[22]

[42] Based on the Quividi Materials, when a person entered the field of view of an IVM's optical sensor, the face detection process followed these steps:

1. An image of the person was captured, temporarily stored in memory (between 66 and 200 milliseconds), and then is processed by Vidi Reports software that is responsible for body and face detection and then overwritten by new images.
2. The body detection process ran the image through an object detection network looking for outlines of body shapes and determined where to position a box around a suspected body shape (i.e. a human body).[23]

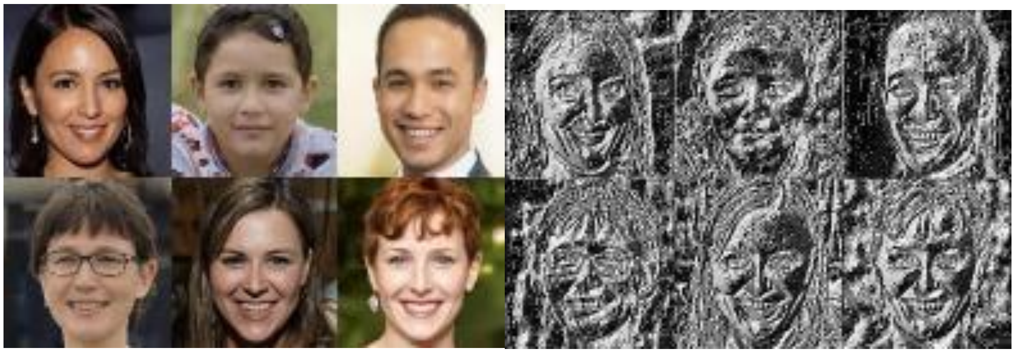
[20] Quividi – FAQ.
[21] Quividi's VidiReports and Biometry.
[22] See footnote 20.
[23] VidiReports uses MobileNetV2 as its backbone, which is a general image classification network trained on a large set of labeled images with over 80 different object categories, including but not limited to human bodies. See (Quividi) Body Detection in VidiReports.

3. At the same time, the face detection process searched the image for "face like" shapes by converting it to a grayscale feature map which was then run through a classifier network.

4. Face detection occurred when a triangular pattern, suggesting the presence of two eyes and a mouth was found, with the output returning the demographic data.

[43] Quividi's VidiReports and Biometry document explains how "the frames produced by the camera are immediately converted into a low-information feature map ..." and provides visual examples of this process immediately below this explanation:

> Quividi's face detection relies on a statistical classifier that operates on **feature images** rather than on visual images; specifically, the frames produced by the camera are immediately converted into a low-information feature map, a transformation that immediately removes most of the fine-level details that could be considered biometric information. Here is an example that shows the input image and, on the right, the actual data processed by the VidiReports:



[43] While it may be true that processing the initial images produced by the IVM camera "removes most of the fine-level details that could be considered biometric information," as illustrated by the low information feature map on the right, I note that the "input images" on the left are examples of clear, personally identifiable images of individuals' faces captured by the IVM camera before the processing and conversion described below.

[44] According to the Quividi Materials, for each person detected by the IVMs, VidiReports generated an audience record and a demographics summary record. The university also advised that a payment record was created for each sale.

[45] The audience record was stored in an encrypted database on the IVMs and consisted of certain data, including:

- "dwell" – the sum of the time a person spends in the camera sensor's field of vision;

- "attention" – the sum of the time the viewer spends on the screen;

- "gender" (optional) – the estimated gender of the person;
- "age" (optional) – the estimated age of the person;
- "mood" (optional) – the person's estimated mood, from very sad to very happy;
- "features" (optional) - presence of beard, mustache, glasses, sunglasses;
- "distance" – the person's average distance from the camera; and
- "num_glances" – the number of times the person looked away from the screen.[24]

[46] The university advised that VidiReports was not set to collect the "features" data.

[47] From the audience record, the demographics summary record captured the data relating to the estimated age range, gender and the total number of viewers observed in front of the IVM.[25] The university advised that this was the only record retained in the Invenda Platform and that the data was aggregated.

[48] Regarding the conversion of recorded facial images into abstract and anonymous numeric descriptors, the university provided this office with a sample motion event record of the abstract numeric descriptors related to a single person's capture by an IVM. This record appeared to take other video frames into account to track observations related to the ongoing motion of people detected in front of the IVM's camera.

[49] Notably, this record contained positioning data for a tracked face, including fixed size and coordinates of face features (contained in fields: height, width, x position and y position). Moreover, it contained face pose data, which consisted of head pose angles and face landmarks.

[50] Based on the foregoing information about the face detection technology, and, in particular, the "input images" from which the low-information feature maps were created, I find in the analysis section below that the use of the IVMs on campus resulted in the collection of personally identifiable images.

Sales and Payment information

[51] To provide the university with sales data and inventory tracking information, the university advised that Adaria installed payment collection software (i.e. smartVend) in the IVMs which accepted payment by credit or debit card, mobile wallets and campus cards.

[52] When a person purchased a snack, the university advised that the card number

[24] Quividi and Privacy Protection.

[25] (Invenda) Demographic Detection Data Schema.

was collected, and that the following transaction data was recorded:

- a timestamp of the payment device confirmation;
- the success or failure of the payment process; and
- the amount of the transaction.

[53] According to the university, this data was stored in the IVMs, sent to the Invenda Platform, and was only used for statistical analysis and reconciling the number of products dispensed with those purchased.

[54] The university advised that Adaria did not store any payment data to reduce security risks related to cardholder information. The university also explained that Adaria's software, which collected payment data, was separate from VidiReports, and that payment data was processed directly between the payment device and the payment service selected by Invenda's customers. Consequently, the university advised that the payment data cannot be matched to the other output records sent to the Invenda Platform and VidiCenter.

Analysis:

Collection of Personal Information

[55] There was no dispute that the IVMs captured video images of individuals' faces on the university 's campus. However, the university argued that the resolution of the optical sensor in the IVMs was too low for the device to be considered a camera or create identifiable images of individuals.

[56] Respectfully, I disagree with the university's position. At the outset, I note that the university did not provide any evidence to support its position.

[57] The Quividi Materials provided by the university itself describe the facial image capturing device as a camera. These materials state that:

> • "each frame from the camera lives solely in the processing unit's volatile memory for a few milliseconds only;"
>
> • "the frames produced by the camera are immediately converted into a low-information feature map;"
>
> • "VidiReports tracks the people it detects but only while they remain in the field of view of the camera"; and

• "if a person exits and re-enters the field of view of the camera, VidiReports will not be able to detect such an event..."[26]

[58] Further, the Quividi Materials describe the IVMs use of a camera sensor or a "webcam":

- "Quividi's VidiReports software uses images from a camera sensor (usually a webcam) and a suite of proprietary real-time image processing algorithms to:
  - detect the presence of human faces in the digital images provided by the camera sensor;
  - estimate the time spent by a detected person in the camera sensor's field of vision and the time spent looking at the screen; and
  - optionally assign a set of anonymous qualifying tags to each detected person, such as gender or age information." [27]

[59] In addition, the university has advised that the optical sensors in the IVMs had resolution of either 1280x720 or 640x480. My review of relevant sources has found that a camera with a 640x480 resolution can capture identifiable images provided the subject is within sufficient proximity.[28] Consequently, a 1280x720 resolution would offer even greater clarity and detail.

[60] In my view, conditions for the cameras or camera sensors to capture identifiable images were favourable because:

- the IVMs were installed indoors, in specific rooms and common areas (such as lobbies and a lounge) areas on the university's campus[29], which likely provided sufficient natural and/or artificial lighting, a factor that typically enhances image clarity;
- the optical sensors were fixed in a static position reducing the chances of motion blur and related image distortion; and

[26] See footnote 21.

[27] See footnote 24.

[28] For example, in the technical paper "Forensic Facial Comparison: Current Status, Limitations, and Future Directions", the authors found that "a minimum horizontal pixel count of 10-16 per face for a known face and 20 pixels for an unknown face is considered the bare minimum for successful identification in frontal view." See https://www.mdpi.com/2079-7737/10/12/1269. Further, in the "Perfect Pixel Count – Meeting your Operational Requirements" report, the authors mapped the horizontal pixels of a face needed to make facial identifications and found that only 20 horizonal pixels were needed. See https://www.axis.com/files/feature_articles/ar_perfect_pixel_count_55971_en_1402_lo.pdf. In the case at hand, the IVMs used a minimum horizontal pixel count of 640.

[29] The locations of the IVMs were set out in a Schedule attached to the Agreement.

- the sensors were likely positioned close to individuals, particularly, in the case of users actively engaging with the machines increasing the likelihood of capturing identifiable images.

[61] Moreover, in my view, it is significant that the Quividi Materials state that face detection by VidiReports "relies on a statistical classifier that operates on feature images rather than on visual images, specifically, the frames produced by the camera are immediately converted into a low-information feature map…"[30]

[62] While Quividi's algorithm enabled removal of biometric information and the conversion of the "frames produced by the camera" into low information feature maps, the existence of this step tends to underscore the fact that the original input images captured by the cameras contained personally identifying information as shown in the examples of photographic input images reproduced in paragraph 43 above.

[63] For these reasons, I find that the resolution of the cameras installed in the IVMs was sufficient to create an identifiable image of an individual.

[64] The university also submitted that no personal information was involved as the images captured by the face detection technology were stored only temporarily for a few milliseconds before being permanently deleted. Therefore, in the university's view, the images did not qualify as *recorded* information about an identifiable individual.

[65] Moreover, as the images were converted into grayscale feature maps that were further converted into numeric descriptors representing an aggregate of the demographic data, the university maintained that none of the output records were about identifiable individuals and, therefore, were not personal information under *FIPPA*.

[66] In support of this position, the university submitted an Officer Certificate from Adaria in which a director certified that Adaria "does not have in its possession or control, biometric personal information (which includes images or videos of faces or people, retinal scans, facial patterns, or facial recognition data) obtained in connection with the Agreement or in connection with any biometric sensors installed in any vending machines serviced by the Company in connection with the Agreement."

[67] The university also provided a copy of a letter they received from MARS and a letter that Adaria received from Invenda, both regarding the IVMs.

[68] MARS' letter stated that the "the Invenda technology used in [the IVMs did] not collect, manage, retain, or process any personally identifiable information" and clarified that the IVMs "[did] not have the capability to capture, retain or transmit imagery."

[69] Invenda's letter, titled "Statement Regarding Demographic Trend Detection

[30] See footnote 21.

Technology," stated:

> As the producer of the Invenda loT solution, the Invenda smart vending machine, and its associated software, we formally warrant that the demographic detection software integrated into the smart vending machine operates entirely locally. It does not engage in storage, communication, or transmission of any imagery or personally identifiable information. The software conducts local processing of digital image maps derived from the USB optical sensor in real-time, without storing such data on permanent memory mediums or transmitting it over the Internet to the Cloud.
>
> The output generated from processing the video stream manifests as a simple file in JSON format…[31]
>
> It is imperative to note that the Invenda Software does not possess the capability to recognize any individual's identity or any other form of personal information.
>
> Further, Invenda's smart vending machines and its software are compliant with General Data Protection Regulation and equivalent data privacy policies.

[70] Despite these letters and the university's submissions, it is clear that the use of the face detection technology in the IVMs resulted in a collection of personal information under *FIPPA*, however transient. As noted above, I was provided with sample facial images captured by the cameras of optical sensor that were of photographic quality, clearly showing individuals' identifiable facial features. These facial images were temporarily stored in memory, even if only for milliseconds, before being sent to VidiReports for processing and conversion to grayscale feature maps and further conversion into numeric descriptors of the individuals' demographic data.

[71] This office has previously held that information collected by video cameras in the nature of personally identifiable images qualifies as personal information under section 2(1) of *FIPPA*.[32]

[72] Pursuant to section 38(1) of *FIPPA*, such information does not need to be permanently recorded to qualify as "personal information." Section 38(1) expands the definition of "personal information" for the purposes of sections 38 and 39 of *FIPPA*, as follows:

[31] JavaScript Object Notation (JSON) is a standard text-based format for representing structured data based on JavaScript object syntax. It is commonly used for transmitting data in web applications.

[32] Privacy Complaint Reports MC10-2 and MC07-68, among others, where this information qualified as "personal information" under paragraph (a) under the definition of "personal information" in section 2(1) of *FIPPA*.

> “personal information” includes information that is not recorded and that is otherwise defined as “personal information” under this Act.

[73] Moreover, I do not accept the university’s claim that VidiReports operated entirely in real-time, as the face detection technology in the IVMs temporarily stored images of individuals’ faces in memory to generate the demographic data and other records. I note that the OPC, the Office of the Information and Privacy Commissioner of Alberta, and the Office of the Information and Privacy Commissioner of British Colombia (the “Commissioners”) reached a similar conclusion in a report of their joint investigation of the Cadillac Fairview Corporation Limited (CFCL) (the Commissioners’ Report)[33].

[74] In that report, the Commissioners assessed whether CFCL was collecting and using personal information without consent through facial detection technology (i.e. Anonymous Video Analytics (AVA)) in mall directories. The Commissioners did not accept CFCL’s assertion that the technology operated solely in real time, noting that facial images were briefly stored during processing[34] and the resulting data that was generated was used afterwards. Despite the short retention period, the Commissioners found this still amounted to a collection of personal information.[35]

[75] I note that an application by plaintiffs to certify a class action against CFCL for the tort of intrusion on seclusion was recently dismissed by the British Columbia Supreme Court in *Cleaver v. Cadillac Fairview Corp. Ltd.*[36] The plaintiff’s’ application was based, in part, on the Commissioners’ Report, which the Court stated could only be admitted for context “but not for the truth of its contents.” Consequently, the contents of the Commissioners’ Report could not be relied on by the plaintiffs or their witnesses. Further, the Court observed that the focus of a certification application “is not on the merits or the weight of the evidence but rather on the appropriate form of the action.”

[76] In considering the criteria for class certification, the Court found no factual basis to demonstrate that the plaintiffs could self-identify as “having viewed a wayfinding directory at one or more of the shopping malls during the relevant periods” and “no rational relationship” between that proposed class definition and the fundamental common issues raised by the plaintiffs.

[77] In case the Court was wrong on that point, it went on to consider whether there was some basis in fact for those common issues, namely, “that a facial image of an individual was recorded and used to create biometric and personal information about that

[33] Joint Investigation of the Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia (“CFCL Report “)

[34] CFCL Report, at para. 48, confirming “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.”

[35] CFCL Report, at paras. 60-63.

[36] 2025 BCSC 910.

individual".

[78] The Court could not consider the plaintiffs' expert testimony as it relied exclusively on the Commissioners' report that was deemed inadmissible for the truth of its content. Therefore, the Court accepted the only evidence before it which was the evidence of an expert retained by CFCL. CFCL's expert attested that the technology in question "takes images ... [of] a face" and that the "captured" facial images were then converted to anonymized "embedding numbers" which could not be used to identify an individual or "to recover the original facial image."[37] While the Court accepted this evidence, it ultimately observed there was "no basis in fact that any facial images were recorded by the cameras located at the Directories." The Court's finding in this respect can only be reconciled with the expert's evidence if it used the word "recorded" to mean "permanently recorded."

[79] In any event, for the purposes of the present investigation, section 38(1) of *FIPPA* does not require personal information to be "recorded" in order to be "collected." Therefore, the issue of whether or not the facial images were "recorded" as a component of the common issues examined by the Court in the class action lawsuit against CFCL, has no bearing on whether personal information in the form of facial images was "collected" within the meaning of *FIPPA*.

[80] Further, where the Court stated "there is no basis in fact for the allegation that the Data contains personal information within the meaning of the relevant statutes," it was not referring to the facial images that were "captured," but rather to the numerical "Data" which the Court defined in its reasons as the "data generated by the Software."

[81] Finally, an application to certify a proceeding as a class action does not involve a trial on the merits, but rather a determination based on admissible evidence that certain certification criteria have been met. The Commissioners' Report was not admissible evidence that could be weighed or tested against other evidence, and, in any event, it was not part of the Court's role to weigh evidence in the certification application. Given the limited use of the Commissioners' Report for context only, the Court's reasons at no point addressed or called into question the Commissioners' finding that "the captured images ... held in memory for a very short period ... represent[ed] a collection of personal information" within the meaning of their respective statutes.

[82] For essentially the same reasons as those in the Commissioners' Report, I find that the capture of images by the face detection technology in the IVMs qualifies as a collection of personal information as defined at section 38(1) of *FIPPA*. Regardless of whether the original image used to create anonymized demographic data was permanently retained in storage, the image was "taken" or "collected" by the equipment's camera and stored for a sufficient period of time to be converted to another format. From any practical perspective, including the perspective of the individual whose facial image

[37] *Ibid*., paras. 42, 43, 49.

was captured, this is a collection of personal information that must find its authority in the provisions of *FIPPA* to be lawful.

[83] As noted above, the university claimed that the IVM software converted recorded facial images into abstract and anonymous numeric descriptors representing an aggregate of the demographic data that could not be linked to any specific individual. The university's claim appears to be confirmed in the published Quividi Materials which state that when VidiReports processes facial images, no data unique to an individual is ever generated, no biometric information is ever extracted, and no recognition or (re)identification is possible.[38] The Quividi materials further state that the audience measurement data generated by VidiReports is "fully anonymous as there is no way to link these data back to a specific person."[39]

[84] Our investigation into this matter has found no evidence to suggest that personal information, beyond the initial temporary capture of facial images, was retained and further used by these vendors.

B. Did the collection of personal information comply with sections 38 and 39 of *FIPPA?*

Authorization to collect personal information

[85] Section 38(2) of *FIPPA* limits the circumstances in which personal information may be collected. This section states:

> No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

[86] In order for an institution to collect personal information in compliance with the requirements of *FIPPA*, one or more of the three criteria specified in section 38(2) must be satisfied. I have not been referred to any statute that could be said to expressly authorize the collection of personal information in this case, nor is there any basis to find that personal information collected by the vending machines was used or intended to be used for the purposes of law enforcement. It therefore falls to be determined whether the collection of the personal information at issue on behalf of the university is necessary for the proper administration of a lawfully authorized activity.

[87] The university is continued as a corporation under section 2 of *The University of Waterloo Act, 1972*,[40] pursuant to which it has "all the property, rights, powers and privileges which it now has, holds, possesses or enjoys" and which, pursuant to section

[38] See footnote 20.
[39] See footnote 24.
[40] The University of Waterloo Act, 1972*,* SO 1972, c 200, ss. 2, 4, 14.1(c), (f).

4, includes “all powers necessary and incidental to the satisfaction and furtherance of its objects as a University.” More specifically, under section 14.1(c) and (f), the Board of Governors of the university has all powers necessary or convenient to perform its duties, which include the power to plan and implement the physical and operational development of the university and to establish and collect fees and charges for academic tuition and for services of any kind which may be offered by the University. Further, pursuant to section 92(1) of the *Legislation Act*, the university has the power as a corporation to contract by its corporate name and to acquire, hold and dispose of personal property.[41]

[88] Given the breadth of the university’s powers, there can be no doubt that the installation and operation of vending machines on the university’s premises as a component of its larger food services operations, and entering into a contract for that purpose, is a lawfully authorized activity. The question remains whether the collection of personal information is necessary for the proper administration of the activity in question, namely the sale of beverages and snacks to members of the public.

[89] The test for determining whether this requirement is satisfied was articulated by the Court of Appeal in *Cash Converters Canada Inc. v. Oshawa (City) ("Cash Converters")* as follows:

> ... [T]he institution must show that each item or class of personal information that is to be collected is necessary to properly administer the lawfully authorized activity. Consequently, where the personal information would merely be helpful to the activity, it is not "necessary" within the meaning of the Act. Similarly, where the purpose can be accomplished another way, the institution is obliged to choose the other route.[42]

[90] As described at paragraph 51 to 54 above, sales from the vending machines involved payment by credit or debit card, mobile wallets and campus cards. The associated payment data was not stored by Adaria but was processed directly between the payment device and the selected payment service in order to reduce security risks related to cardholder information. Further this information was kept separate from VidiReports and the sales and inventory tracking data. It therefore appears that the collection of personal cardholder information in connection with the payment process was no more than necessary for the purposes of processing each transaction and, in my view, satisfied the test articulated in *Cash Converters*.

[91] In contrast, I have been provided with no evidence or argument by the university, nor am I aware of any facts or circumstances, by which the collection of a facial images by the IVMs for conversion to demographic data is necessary for operation of the machines or the completion on individual transactions. While the collection and conversion of facial images may be helpful to enable vendors to better understand the

[41] Legislation Act, 2006, S.O. 2006, c. 21, Sched. F, s. 92(1).

[42] 2007 ONCA 502, at para. 40.

demographics of the population they serve and to track sales and adjust inventories, any benefit from collecting that information is at best merely helpful, and not necessary to administer a lawfully authorized activity.

[92] My findings in this regard stand in contrast to the IPC's 2024 McMaster University Privacy Complaint Report[43] which examined the use of online proctoring software by McMaster to capture audio and video recordings of students who were taking their exams remotely during the Covid pandemic. In the absence of direct human oversight, the recording function of this online proctoring service gave instructors the ability to review first-hand any exam sessions in which the technology flagged suspicious behaviour consistent with cheating. In this circumstance, the individual items and classes of personal information collected by the software on behalf of the university were necessary for the purpose of conducting and proctoring the exams.

[93] As a result, the Commissioner was satisfied in that case that the collection of personal information by the proctoring software was "necessary" within the meaning of section 38(2) for the proper administration of the university's lawfully authorized activity of conducting and proctoring online exams during the pandemic, and in other circumstances that could be justified post-pandemic.[44]

[94] The collection of facial images through the university's use of the IVMs' facial detection technology falls far short of the necessity test articulated in *Cash Converters* and found to be satisfied in the McMaster Report.

[95] Accordingly, I find that the collection of facial images by the IVMs was not expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity, and thus was not in compliance with section 38(2) and amounted to a privacy breach.

Notice of collection

[96] Subject to exceptions[45], none of which applies in this case, section 39(2) of *FIPPA* requires that individuals be informed when their personal information is being collected. This section states:

> Where personal information is collected on behalf of an institution, the head shall, unless notice is waived by the responsible minister, inform the individual to whom the information relates of,

[43] Privacy Complaint Report PI21-00001

[44] *Ibid*, paras. 58-61. It is noteworthy that the Commissioner expressed ongoing reservations about the use of online proctoring technology in conjunction with artificial intelligence technologies and the need to develop privacy protective guardrails in this connection.

[45] Under section 39(2), the responsible minister (the Chairman of the Management Board of Cabinet) may waive the notice requirement and section 39(3) of *FIPPA* sets out exceptions.

> (a) the legal authority for the collection;
>
> (b) the principal purpose or purposes for which the personal information is intended to be used; and
>
> (c) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

[97] The notice required by section 39(2) may be provided orally, in writing or in any manner that meaningfully informs the individual.[46]

[98] In this matter, the university did not inform individuals that the IVMs were using face detection technology that captured their images. As a result, the affected individuals were not given the opportunity to avoid the collection of their personal information either by choosing not to use the machines or by avoiding coming within their camera range. They were also not given any of the required information under section 39(2).

[99] In light of my finding above that the collection of personal information in the form of identifiable facial images was not in accordance with section 38(2), the university could not have provided notice of the legal authority for the collection in compliance with section 39(2).

[100] I note that in its sales-related materials, Quividi encourages its end users "to adopt best practices for transparency to ensure individuals are well-informed about data collection activities and associated purposes."[47] To that end, Quividi recommends that these users:

- "Place conspicuous disclosure stickers on premises where screens are located or directly on the screens, ensuring visibility to visitors; and
- Use easily understandable language on these stickers, maintaining clarity for a broad audience's comprehension."[48]

[101] I have been provided with no information explaining why the university was not made more explicitly aware of Quividi's transparency best practices in the procurement process through the supply chain from Invenda, MARS and Adaria.

[102] Had the university known of Quividi's transparency recommendation, the university would have been made aware of the technical features of the IVMs, including its data collection activities and associated purposes. With this knowledge, the university may have been better positioned to reassess its procurement decision given its obligation to

[46] IPC Practices No. 8 Providing Notice of Collection and page 12 of the IPC's "Guidelines for the Use of Video Surveillance, October 2015", both available on the IPC's website.

[47] See footnote 20.

[48] See footnote 20.

comply with section 38(2) of *FIPPA*, which prohibits the collection of personal information that is not necessary for the proper administration of any lawfully authorized activity carried out by the university.

[103] Even if the university could be said to have legal authority to collect facial images of users of the IVMs (which I find it did not), the university did not provide any meaningful notice of such collection in accordance with the requirements of section 39(2). In fact, it provided no such notice at all.

[104] In conclusion, I find that the university did not, and could not, provide notice of the collection of personal information in accordance with section 39(2) of *FIPPA*.

C. Did the university have reasonable measures in place to protect personal information in accordance with section 4(1) of Regulation 460 under *FIPPA*?

[105] *FIPPA* requires that institutions protect personal information that they hold or that is collected and held on their behalf.[49]

[106] This is especially important when institutions work with third parties who may collect or access personal information.[50] A third-party can be any outside person, business, or organization that provides a service to or works for an institution.[51]

[107] Accordingly, when institutions contract with third parties, they must still follow *FIPPA* and, therefore, they need contractual and oversight measures in place to ensure compliance with this legislation.[52]

[108] Regulation 460, made under *FIPPA*, establishes rules for the security of records that an institution has. Specifically, section 4(1) of Regulation 460 states:

> Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

[109] These requirements "appl[y] throughout the life-cycle of a given record, from the point at which it is collected or otherwise obtained, through all of its uses, and up to and including its eventual disposal."[53] Also, "reasonable measures" do not need to cover every possible scenario to prevent authorized access; rather, they need to be "fair and suitable under the circumstances".[54]

[49] See Part III Protection of Individual Privacy of *FIPPA*.
[50] IPC Practice No. 18 "How to Protect Personal Information in the Custody of a Third Party".
[51] See footnote 47.
[52] *Ontario Criminal Code Review Board v. Hale*, 47 O.R. (3d) 201 (C.A.) and Privacy Complaint Report PR16-40.
[53] Privacy Complaint Report MI10-5.
[54] Investigation Report I93-044M.

[110] In Privacy Complaint Report PR16-40, the investigator noted that section 4(1) of Regulation 460 does not prescribe a "one-size-fits-all" approach to security:

> It does not set out a list of measures that every institution must put in place regardless of circumstance. Instead, it requires institutions to have "reasonable" measures and ties those measures to the "nature" of the records to be protected. It follows that the same security measures may not be required of all institutions. Depending on the nature of the records to be protected, including their sensitivity, level of risk and the types of threats posed to them, the required measures may differ among institutions.

[111] In this matter, the third-party service provider was Adaria with whom the university had contracted to provide snack vending services.

[112] Accordingly, I must determine whether the university had reasonable measures in place to protect any personal information that may have been involved in the provision of these services.

[113] As part of my investigation, I reviewed copies of the university's snack vending services Request For Proposal (the RFP), Adaria's proposal in response to the RFP (Adaria's Proposal) and the Agreement.

[114] In assessing these documents, I considered the IPC's "Privacy and Access in Public Sector Contracting with Third Party Service Providers" guidance document which sets out best practices for ensuring privacy when preparing for and entering into agreements with service providers. [55]I also considered the IPC's "Planning for Success: Privacy Impact Assessment Guide" which assists institutions in conducting a privacy impact assessment (PIA) to assess compliance with *FIPPA*.

[115] Below, I find that the university may have had reasonable contractual measures in place in so far as it required Adaria, through what appears to be standard-type provisions, to protect any personal information involved in the delivery of the snack vending machines. These contractual provisions were included despite the university's assertion that it was not aware of any personal information being collected as part of the face detection technology embedded in the IVMs.

[116] However, beyond the written agreement, it was the university's overall procurement process for the RFP that failed to identify and assess the privacy implications of this technology offered by its third-party service provider and their suppliers. Specifically, the university's procurement process did not engage the level of due diligence necessary to uncover the fact that the technology being offered by Adaria involved the

[55] https://www.ipc.on.ca/en/resources/privacy-and-access-public-sector-contracting-third-party-service-providers

collection of visual images of IVM users, contrary to section 38(2) of *FIPPA*.

The University's Vendor Management Program

[117] The university advised that it had a vendor management program in place to safeguard the personal information of individuals on campus prior to the installation of the IVMs.

[118] The university also advised that when a department seeks to implement a new business process or redesign an existing process or service involving a substantial change to the processing of personal information, it is required to complete an Information Risk Assessment (IRA) based on IPC guidance. [56]

[119] These requirements involve completing an IRA intake questionnaire for review by the university's Privacy Officer and Information Security Officer, who provide recommendations on privacy protection and data security.

[120] The university's IRA program aims to:

1. Identify and understand privacy and security risks associated with new or redesigned university processes or services that use sensitive information, including personal information.

2. Prevent or reduce privacy and security issues.

3. Enhance privacy and security protection.

4. Help Information Stewards decide whether to move forward with the initiative.[57]

[121] Where the university decides to complete an IRA as part of its procurement process, the questionnaire includes the following two questions:[58]

- Will it involve use of new technology, or one known to impact privacy that could raise significant privacy risks (e.g., biometrics, smart cards, drug testing, or technology with surveillance capabilities)?

- Will it involve creation or modification of databases that will contain Restricted or Highly Restricted Information, including Personal Information? In particular, where the data is sensitive or relates to a significant number of people, or that will link separate databases or create files that index or point to Personal Information on such databases?

[56] Information Risk Assessment | Information and Privacy | University of Waterloo: https://uwaterloo.ca/privacy/information-risk-assessment.

[57] See footnote 56.

[58] See footnote 56.

[122] The university advised that typically, their Procurement Department, in consultation with the department that is to work with the vendor, prepares the request for proposal for vendors handling personal information. The university also advised that recommendations from this IRA process, when undertaken, are included in the proposal.

[123] In this case, the university advised that the Procurement and Food Services departments created the RFP and that it contained all the standard personal information and data security requirements found in the university's requests for proposals. However, the university advised that they did not complete an IRA as part of the procurement process for the IVMs because they believed that only payment card and related financial information would be collected. As such, the department did not anticipate any significant change in how personal information was being processed.

The RFP, Adaria's Proposal and the Agreement

[124] The RFP was posted in June 2023, and the successful respondent was responsible for providing and maintaining vending services on the university's campus.

[125] The RFP informed respondents that the university must handle protected information in accordance with *FIPPA*. It also stated that the successful respondent, upon entering into an agreement and handling protected information, would be required to provide details on their data protection practices. The contract would only be awarded if the university was satisfied with these practices.

[126] Further, the RFP required that respondents provide security documents, such as information security policy, data privacy policy, incident response plan, diagrams showing the flow of personal or sensitive information, audit reports and security certifications. It also required that they provide a "[d]escription of the roles and responsibilities of any additional agents and sub-contractors who will be involved in providing the Snack Vending Services".

[127] With respect to data, the RFP noted that it was important for the "Food Services management team to have just-in-time information on the performance of [their] Snack Vending business with accurate accountability to sales and volumetric reporting" and required that bidders provide "reporting on volume and sales per machine location."

[128] Regarding the IVMs, the RFP specifically asked respondents to "include a photo or catalogue image of the type of Snack Vending machines to be provided to the [university], including the SKU number of the equipment and its specifications" and "[o]utline the technologies to be proposed including technology used to manage inventory levels". Further, for each SKU model, respondents had to provide information about its data or network requirements.

[129] Adaria's Proposal informed the university that it had "partnered with Mars, Frito-Lay to test product innovations at vending machines" and that MARS Intelligent Vending Machines would be installed. The proposal stated that MARS was "implementing their

new Intelligent Mars Machines and we are working with Mars on this deployment in Canada." It also included a brochure on these machines indicating that they required "High Traffic/Dwell Time."

[130] Regarding the technology in the machines, Adaria's Proposal stated:

> ...we have implemented a proprietary remote monitoring system, utilized on all vending equipment we deploy. This is a miniature device that is fitted into vending machines and transmits sales data to our backend servers, which processes the information into online reports that we use to replenish our machines more efficiently.

[131] The proposal explained that this remote monitoring system (i.e. smartVend) "is an in-house developed telemetry system that provides accurate sales data and item-level inventory tracking of all deployed vending machines."

[132] Adaria's Proposal also stated that they "will not use any additional agents or subcontractors to perform the requirements of [the] RFP".

[133] Under the Agreement, the university owned all personal information "submitted to or created by" Adaria, who agreed to handle it in compliance with all applicable privacy laws. The Agreement specifically required the university, Adaria and Adaria's agents and subcontractors to handle and protect personal information in compliance with *FIPPA*. It also defined "personal information/data" to include the definition of "personal information" under *FIPPA*."

[134] Before disclosing any confidential information due to legal requirements or government requests, the Agreement required Adaria to notify the university, giving it the chance to prevent or limit the disclosure The Agreement also required that Adaria, along with its agents and subcontractors, continue protecting confidential information even after the Agreement ends.

[135] The Agreement included comprehensive security provisions requiring Adaria to implement appropriate safeguards and security controls to protect personal information from unauthorized or malicious use, as well as maintain a formal security and breach incident response program.

[136] When the Agreement ends, Adaria and its agents and subcontractors would be required to return all data (including confidential information) to the university. They were also required to permanently destroy all digital copies of the data in a way that made recovery impossible and provide written confirmation that this was done.

[137] Finally, under the Agreement, the university had the discretion to hire a qualified third party to conduct information security audits.

Analysis

[138] In Privacy Investigation Report PC12-39 and Privacy Complaint Report PR16-40, this office considered relevant contractual provisions for determining whether an institution met its obligations to ensure that all reasonable steps were taken to protect the privacy and security of personal information under its control in accordance with section 4(1) of Regulation 460. These provisions include:

- Ownership of data
- Collection, Use, and Disclosure
- Confidential Information
- Notice of Compelled Disclosure
- Subcontracting
- Security
- Retention and Destruction
- Audits

[139] In this matter, the Agreement appears to have contained all the appropriate standard clauses necessary to protect personal information involved in the delivery of snack vending services by Adaria.

[140] Despite the apparent adequacy of these contractual measures to protect any personal information collected, the fact remains that the collection of personal information through the IVMs' face detection system was not authorized.

[141] As mentioned above, the university was not aware that the IVMs contained face detection technology that collected personal information. Based on the Officer Certificate from Adaria, it appears that they too were unaware of this collection. It was only after an IVM malfunctioned on campus that the university became aware that data was being collected and accessed by Invenda and Quividi.

[142] The RFP did not request vending machines that use face detection technology to collect personal information or provide demographic data analytics. Further Adaria's Proposal did not explicitly refer to the face detection technology in the IVMs or indicate that additional agents or subcontractors would be used to fulfill the RFP's requirements.

[143] However, Adaria's Proposal did inform the university of Adaria's collaboration with MARS to test product innovations and that new MARS Intelligent Vending Machines would be installed that required high traffic and/or dwell time. (i.e. a lot of people passing by and/or lingering around the machines).

[144] The university advised that an IRA was not completed because it did not anticipate a significant change in the processing of personal information based on the belief that only financial information would be collected by the IVMs. However, given that Adaria's Proposal informed the university that it would be working with MARS to implement and deploy new intelligent MARS machines in Canada, this should have caught the attention of the university and alerted it to the possible privacy implications necessitating further scrutiny.

[145] Accordingly, if the university had conducted an IRA during its procurement and tendering processes, it likely would have identified key red flags, specifically, that the machines used new innovative technology with surveillance capabilities involving a significant number of people.

[146] In my view, doing so would have highlighted and prevented, or mitigated, the risk of the unauthorized collection of personally identifiable images that occurred on the university's campus.

[147] This omission highlights the importance of having not only good contractual templates in place, but also sound and robust information management practices throughout the entire procurement process, from planning, tendering, vendor selection, contracting, agreement management, right up to and including termination.

[148] Regarding procurement planning, the IPC's Contracting with Third Party Service Providers Guide advises that institutions should, among other things, consider:

- *Defining the records* to develop a clear understanding whether personal information will be involved in the procurement project or initiative; and
- *identifying and mitigating privacy and security risks* (using a privacy impact assessment) before starting the procurement process or signing an agreement and creating measures to mitigate them, as well as consider whether the service provider should also conduct a security assessment of its services, processes or technology before entering into the agreement.

[149] The IPC's Contracting with Third Party Service Providers Guide also recommends that institutions define the types of records and personal information the service provider will have access to and be responsible for processing, building upon this step taken during procurement planning.

[150] Further, while the IPC's PIA Assessment Guide notes that a PIA is not required where an institution determines that a project will not involve personal information, it also recommends that this conclusion and the reasoning behind it be documented.[59] In this matter I was not provided with any information regarding the university's conclusions

[59] See page 5 in the IPC's PIA Assessment Guide.

or rationale for not conducting a PIA in relation to the RFP.

[151] Finally, although the RFP required bidders to describe the technologies proposed for use in the vending machines and provide details about each machine's data or network requirements, it did not require bidders to conduct a security assessment of the technology to be implemented in the machines.

[152] In my view, had Adaria conducted a PIA during the procurement process for the RFP, it would have evaluated the technology used in the new IVMs to be deployed by MARS in Canada and likely identified that this technology involved Invenda, Quividi and VidiReports, and the associated risk of unauthorized collection of personally identifiable images.

[153] Moreover, regarding the tendering process, the IPC's Contracting with Third Party Service Providers Guide recommends that institutions "[u]ndertake any activities required to collect sufficient information to evaluate service providers." Since the university did not conduct an IRA or PIA, or request that Adaria do so, the university failed to gather enough information to assess whether Adaria's service delivery would comply with *FIPPA*.

[154] Based on the above, I find that although the university had reasonable contractual measures in place with Adaria to ensure the privacy and security of personal information under its control, it failed to carry out the necessary due diligence to uncover the fact that the delivery of IVM services it was contracting for would involve the collection of personal information contrary to *FIPPA*.

[155] Accordingly, I find that the university was deficient in its procurement process by failing to conduct an IRA or PIA, or requiring that Adaria do so, considering the information provided in the Adaria Proposal.

[156] Because of this deficiency, the university missed key red flags relating to the technology used in the IVMs indicating that there was a potential privacy risk. It also failed to gather sufficient information to properly evaluate the third-party service providers and their suppliers. These deficiencies resulted in the university being unaware of the face detection technology in the IVMs that collected personally identifiable images without authorization.

[157] Shortly after the software error appeared on the IVM, and immediately upon becoming aware of the face detection technology in the IVMs, the university disabled the face detection software and removed all IVMs from its campus. The university also received assurances from Invenda that all the collected data, including data generated in processing the images, has been permanently deleted.

[158] Although the risks associated with the continuing use of the IVMs have now been averted, there are several recommendations I am making to the university to avoid such a situation from recurring in the future.

[159] Specifically, when planning to enter into an agreement with a third party vendor in the future, that may involve the deployment of new "smart" technologies, I recommend that the university conduct a PIA (or IRA in this case) and also require that prospective third-party service providers do the same as part of their procurement process. While this stands as a recommendation today, the requirement to conduct a PIA in similar circumstances will become both explicit and mandatory under recent changes to *FIPPA* that are set to take effect as of July 1, 2025.

[160] I also recommend that the university not only include appropriate privacy and security-related clauses in its agreements with third party vendors, but that it follow the IPC Guidance on Contracting with Third Party Service Providers to ensure that it identifies, assesses and mitigates any potential risks to personal information throughout the entire procurement process, including during the planning, tendering, vendor selection, agreement management and termination phases.

CONCLUSIONS:

Based on the results of the investigation, I have reached the following conclusions:

1. The university's use of face detection technology resulted in a collection of "personal information" within the meaning of section 2(1) and section 38(1) of *FIPPA*.

2. The collection of personal information was contrary to section 38(2) of *FIPPA*.

3. The university did not, and could not, provide notice of the collection of personal information as required by section 39(2) of *FIPPA*.

4. The university had reasonable contractual measures in place with its third-party service provider to ensure the privacy and security of personal information under its control.

5. However, the university was deficient in its overall procurement process by failing to identify that personal information would be collected as part of the IVM services it was contracting for contrary to section 38(2) of *FIPPA*. This failure resulted in an inability to properly evaluate the third-party service providers and their suppliers and make an appropriate selection. As such, the university fell short of its obligation to protect the personal information under its control in accordance with section 4(1) of Regulation 460.

RECOMMENDATIONS:

Given the conclusions reached in this investigation, I make the following recommendations, which the university has agreed to implement:

1. The university should review its privacy policies to ensure that any future collection of personal information complies with sections 38(2) and 39(2) of *FIPPA*.

2. When planning to enter into agreements with third-party service providers, particularly those involving the use of new or "smart" technologies, the university should ensure that it carries out the necessary due diligence to identify, assess and mitigate any potential risks to personal information throughout the entire procurement process, including during the planning, tendering, vendor selection, agreement management and termination phases.

   This includes conducting a PIA and/or requiring the third-party service provider do so as part of its procurement process where appropriate, following the IPC Guidance on Contracting with Third Party Service Providers, as well as including appropriate standard privacy and security clauses in all contracts with third-party vendors.

Original Signed by: June 11, 2025

John Gayle
Investigator