



Information and Privacy  
Commissioner/Ontario  
Commissaire à l'information  
et à la protection de la vie privée/Ontario

---

---

# **INVESTIGATION REPORT**

**INVESTIGATION PC-010005-1**

**Alcohol and Gaming Commission of Ontario**

---

---

February 26, 2001

# THE USE OF BIOMETRIC FACE RECOGNITION TECHNOLOGY IN ONTARIO CASINOS

## INTRODUCTION

### Background of the Investigation

On January 15, 2001, the Office of the Information and Privacy Commissioner (IPC) was contacted by a reporter from the *Hamilton Spectator*, who was seeking information about the use of biometric face recognition technology by the Ontario Provincial Police (OPP) in Ontario casinos. The *Spectator* and other media subsequently reported that the OPP was secretly scanning the faces of customers at all Ontario casinos for comparison to “mug shots” in a police database.

On January 16, 2001, the Commissioner launched an investigation into the use of face recognition technology at Ontario casinos. We immediately contacted the Alcohol and Gaming Commission of Ontario (AGCO), an independent agency reporting to the Minister of Consumer and Business Services, responsible for regulating liquor licensing and gaming control in the province.

Our investigation unfolded as follows:

- On the afternoon of January 16, 2001, we held an initial fact-finding meeting with an AGCO staff member and two OPP officers seconded to the AGCO’s Investigations Branch.
- On January 17, 2001, the Commissioner had a telephone conversation with Duncan Brown, Chief Executive Officer of the AGCO, to discuss her concerns.
- On January 17, 2001, we also met with representatives from Biometrica Systems, Inc., a U.S.-based company that provides the OPP with the face recognition technology used, including search, direct video input, and local database creation tools (“Visual Casino”); a database of known and suspected casino cheats (“Casino Information Database”); and access to a computer network that enables North American casinos to rapidly send information to each other (“Casino Information Network”).
- On January 18, 2001, we sent a letter to Mr. Brown requesting that his agency provide written responses to a list of questions relating to our investigation into the AGCO’s use of face recognition technology.
- On January 29, 2001, we received a letter from the AGCO with written responses to our questions.
- On February 6, 2001, the Commissioner and two staff members inspected the OPP surveillance activities relating to the use of face recognition technology at “Casino Niagara” in Niagara Falls, one of the three commercial casinos in Ontario.

Throughout the course of our investigation, we received the full and complete cooperation of the AGCO and the OPP.

### **Face Recognition Technology**

The face recognition system used by the OPP is a form of biometric technology. A biometric is a unique, measurable, physiological characteristic or trait of a human being used for automatically recognizing or verifying identity. Other forms of biometric technology include finger scanning, iris recognition, retinal scanning, hand geometry, voice recognition and signature recognition.

Face recognition technology attempts to mimic the way in which people recognize each other by using computer algorithms to simulate human interpretations of the face. Many current technologies use either video or thermal imaging to capture a still image of a person's face. The face recognition software scans the face and translates spatial relationships between various parts of the face into a unique numeric template, which is compared to a database for matching purposes.

### **Findings of Fact**

The Investigations Branch of the AGCO is responsible for ensuring that gaming in Ontario casinos is conducted honestly and is free from criminal activity. The branch is comprised mainly of seconded OPP officers, who have a round-the-clock presence at three commercial casinos (Casino Windsor, Casino Niagara, Casino Rama) and five charity casinos (Sault Ste. Marie, Brantford, Thunder Bay, Point Edward, Great Blue Heron – Port Perry). These officers are primarily responsible for enforcing section 209 of the *Criminal Code*, which creates an indictable offence for cheating while playing a game or betting, commonly referred to as a “cheat at play.” The OPP operates separate and apart from the security and surveillance services that casinos are required to provide under the *Gaming Control Act* regulations.

The OPP has been using face recognition technology at Ontario casinos since May 2000. The technology is not used at racetrack slot machine facilities.

The OPP officers assigned to casino surveillance receive special training on how games of chance are played and on an extensive number of methods of cheating at games. All OPP officers authorized to use the face recognition system also receive a full day of training from Biometrica Systems, Inc.

OPP officers use video surveillance to monitor the activities of suspicious casino patrons. If an officer has a reasonable suspicion that an individual is engaging in criminal activity, he or she may then decide to use the face recognition software to determine if the individual in question is a known or suspected casino cheat.

The officer diverts the video feed of the suspect into the face recognition software, which displays the streaming video on a computer screen. Next, the officer freezes the video feed to produce a “live portrait” or still image of the suspect's face. The officer then scans the biometric

features of the suspect's face, which produces a numeric template. This template is then compared for matching purposes against two databases.

The Casino Information Database contains approximately 800 faces of known and suspected casino cheats throughout North America and is supplied by Biometrica Systems, Inc. The OPP surveillance team at each casino also maintains its own, separate database, which contains the faces of casino cheats convicted in Ontario and individuals subject to ongoing law enforcement investigations for allegedly cheating at play in Ontario casinos. The facial scans are not compared to information contained in any other criminal databases, most notably CPIC (Canadian Police Information Centre), a national computer-based police information system.

Whenever the face recognition system is used, an officer must prepare an incident report, which is reviewed by a supervising officer. Only if an investigation concludes that a person has engaged in illegal activity will the facial scan be retained in the OPP database at that particular casino. If an investigation concludes that a person was not involved in any illegal activity, the facial scan is deleted and no copy is maintained on file.

If an individual is charged and convicted of a cheat at play under section 209 of the *Criminal Code*, the court may issue an order or conditions of probation that prohibit that individual from entering any casinos in Ontario. In such cases, the OPP team at the casino where the individual was arrested may send the facial scan to OPP teams at other casinos in the province for inclusion in their databases. However, if an individual is acquitted, the facial scan is then deleted in its entirety and no copy is maintained on file.

The OPP teams at each Ontario casino are also connected to the Casino Information Network, an online system that enables casinos across North America to rapidly send information to each other. However, the network is used primarily in U.S. cities with multiple casinos. For example, a casino in Las Vegas that has expelled an individual for allegedly cheating can use the network to quickly send information about that individual to other local casinos. Although the OPP teams at Ontario casinos occasionally receive information over the network, they do not send their facial scans to law enforcement agencies and casinos in other jurisdictions or to Biometrica Systems, Inc.

Some media reports had suggested that the OPP was scanning the faces of all casino patrons. This is not the case. Our investigation found that OPP officers do not engage in this practice; namely, they do not scan the face of every person who enters a casino. On the day of our visit to Casino Niagara, we found that there were less than 40 scans maintained in the OPP database at that particular casino. In addition, the total number of facial scans contained in the eight OPP databases over the eight Ontario casinos number fewer than 200, which represents approximately five scans for every million casino patrons.

The limited scanning undertaken by the OPP is in marked contrast to the rapid, person-by-person scanning recently employed by the Tampa Police Department in Florida before the 2001 Super Bowl. On the day of the game, the faces of an estimated 100,000 fans and workers who passed through the football stadium turnstiles were digitally scanned and covertly compared to an extensive, customized database of known felons, terrorists, and con artists provided by local,

state, and federal law enforcement agencies, all without notice. The American Civil Liberties Union (ACLU) has called for public hearings on the use of security systems that may jeopardize the public's right to privacy.

The OPP surveillance centres are found in parts of the casino that are not accessible to the public. Access is limited through the use of locked doors and card-scanning devices. In addition, only those OPP officers who are assigned to casino surveillance have access to the face recognition system and the databases of known and suspected criminals. Access to the face recognition system is password-controlled, meaning that only authorized OPP officers are permitted to gain entry into the system.

### **Issues Arising from the Investigation**

The following issues were identified as arising from this investigation:

(A) Is the information in question “personal information” as defined in section 2(1) of the *Freedom of Information and Protection of Privacy Act* (the *Act*)?

(B) Is the OPP collecting personal information in compliance with section 38(2) of the *Act*?

(C) Is the AGCO providing proper notice, under section 39(2) of the *Act*, of the collection of personal information?

(D) Is the OPP’s use of the personal information in compliance with section 41 of the *Act*?

### **RESULTS OF THE INVESTIGATION**

#### **Issue A: Is the information in question “personal information” as defined in section 2(1) of the *Freedom of Information and Protection of Privacy Act*?**

Section 2(1) of the *Act* states, in part, that “personal information” means recorded information about an identifiable individual, including,

- (a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual.

In our view, the still images of suspects that are retained by OPP officers constitute the personal information of those individuals. Under section 2(1) of the *Act*, a “record” means any record of information however recorded, whether in printed form, on film, by electronic means or otherwise, including a photograph. If an OPP officer concludes that a suspect is engaging in illegal activity and decides to store a still image of the suspect’s face, the officer is recording information about that particular individual by electronic means. Thus, the still image that is stored is “recorded” information.

The information collected must also be about an “identifiable individual.” OPP officers use face recognition technology for identification purposes. They are endeavouring to identify a suspect by comparing his or her facial biometrics to databases of known or suspected cheats. Consequently, since the still images may serve to identify an individual, we consider them to be about an “identifiable individual.”

The still image also displays significant physical characteristics about that individual, including his or her race, colour, age, and sex. Thus, the stored images of suspects meet the requirements of paragraph (a) of the definition of “personal information” in section 2(1) of the *Act*.

Conclusion: The information collected by the OPP through the use of face recognition technology is “personal information” as defined in section 2(1) of the *Act*.

**Issue B: Is the OPP collecting personal information in compliance with section 38(2) of the *Act*?**

Section 38(2) of the *Act* prohibits the collection of personal information 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.

In our view, the OPP officers assigned to casino surveillance collect personal information about suspects for the purposes of law enforcement. Law enforcement is defined in section 2(1) of the *Act* as:

(a) policing,

(b) investigations or inspections that could lead to proceedings in a court or tribunal if a penalty or sanction could be imposed in those proceedings, and

(c) the conduct of proceedings referred to in clause (b);

The AGCO submits that OPP officers who work in casinos gather information pursuant to the duties set out in section 42 of the *Police Services Act*, R.S.O. 1990, c. P.15, as amended. These duties include preventing crimes and other offences; apprehending criminals and others who may lawfully be taken into custody; and laying charges and participating in prosecutions. OPP officers seek to prevent gaming-related crimes; apprehend criminals who violate section 209 of the *Criminal Code*; and lay charges against and participate in the prosecution of such individuals. These duties are all essential components of “policing.”

Moreover, under section 209 of the *Criminal Code*, a cheat at play is an indictable offence punishable by up to two years in prison. In other words, an investigation undertaken by OPP officers could lead to proceedings in a court of law, and a penalty or sanction could be imposed in those proceedings. Thus, the activities of OPP officers assigned to casinos fall within the definition of “law enforcement.”

The AGCO and OPP have assured us that any personal information collected through the application of face recognition technology is used solely for the purposes of law enforcement. If an investigation concludes that a person has engaged in illegal activity, the facial scan is retained in the OPP database at that particular casino. If an investigation concludes that an individual is not involved in illegal activity, the facial scan is deleted. The personal information is not used for any other secondary purpose beyond law enforcement. More specifically, access by OPP officers is restricted to those working on casino law enforcement and only for that purpose.

Conclusion: The OPP's collection of personal information is in compliance with section 38(2) of the *Act*.

**Issue C: Is the AGCO providing proper notice, under section 39(2) of the *Act*, of the collection of personal information?**

Section 39(2) of the *Act* states that:

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,

- (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.

The three commercial casinos and five charity casinos have posted signs that notify patrons that video surveillance is used on their premises. For example, a sign posted at the entrance of Casino Niagara reads as follows: "Some areas monitored by video surveillance." However, these signs do not notify patrons that their personal information may also be collected through the use of face recognition technology, nor do they adhere to all three requirements set out in section 39(2) of the *Act*.

With respect to the use of face recognition technology, the AGCO submits that section 39(3) of the *Act* applies because the face recognition system is an investigative tool used by seconded OPP officers in carrying out their duties. Section 39(3) of the *Act* provides an exemption to the notice requirement in section 39(2):

Subsection (2) does not apply where the head may refuse to disclose the personal information under section 14(1) or (2) (law enforcement).

In this particular situation, we believe that the only parts of subsections 14(1) or (2) that could possibly apply to exempt the institution from the requirement to provide notice are subsections 14(1)(a), (b) and (c):

A head may refuse to disclose a record where the disclosure could reasonably be expected to,

(a) interfere with a law enforcement matter;

(b) interfere with an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result;

(c) reveal investigative techniques and procedures currently in use or likely to be used in law enforcement;

The AGCO submits that because the face recognition system is only used if there is an ongoing police investigation, it is difficult to imagine a situation where the head would not refuse access to facial scans under either subsections 14(1)(a) or (b). During an ongoing investigation, the facial scan of a suspect may be retained in the OPP database at that particular casino until the investigation is concluded.

The AGCO submits that the *Act* does not require the provision of a general notice. It argues that even in cases where a person's face is scanned and later deleted from the database, because the person was not found to have been involved in any wrongdoing, the biometric system is being used solely as an investigative tool, bringing the activity within section 39(3), the exception to section 39(2). Thus, the AGCO argues that this type of activity does not attract a requirement to notify the general public.

In relation to section 14(1)(c), the AGCO submits that it is preferable to avoid giving notice because doing so would reveal a confidential investigative technique: "The matter of biometric scanning has been in the press and we understand that the use of these systems is known to professional casino cheaters, however, it is still not known by many small-time cheaters. From an enforcement perspective, it would be preferable to avoid giving notice that biometric systems are in use."

We have considered the views of the AGCO and the interpretation given to the notice provision. We accept that the provision is capable of more than one interpretation and that the AGCO's view is one that could be taken. However, we prefer another interpretation of the notice provision, for the reasons set out below.

We accept that disclosing the facial scan of a specific, suspected casino cheat during the course of an investigation could reasonably be expected to interfere with a law enforcement matter or an investigation under subsections 14(1)(a) and (b). Thus, in those circumstances, the OPP would not be required to notify a specific individual that it was using face recognition technology to collect his or her personal information.

However, in order to fall within the section 39(3) exemption from the notice requirement, the head must be in a situation where he or she could "refuse to disclose the personal information under section 14(1) or (2)." These provisions are not blanket exemptions but incorporate injury



elements. The head must demonstrate that disclosure of a record could reasonably be expected to cause harm to an ongoing law enforcement matter or investigation.

In our view, subsections 14(1)(a) and (b) would not apply to exempt an institution from a requirement for a general notice to inform members of the public who are entering a casino that the OPP may be collecting their personal information through the use of face recognition technology. We do not believe that such a notice could reasonably be expected to interfere with a law enforcement matter or interfere with an investigation undertaken with a view to a law enforcement proceeding or from which a law enforcement proceeding is likely to result. An individual's face displays unique and highly personal information about that individual, including his or her race, colour, age, and sex. In our view, members of the public should be made aware that this information could be collected if they choose to enter a casino in Ontario.

Moreover, as noted above, the OPP database at each casino includes the facial scans of persons subject to ongoing law enforcement investigations. If an OPP officer concludes that an individual has not engaged in any illegal activity, the scan is completely deleted, with no copy maintained on file. However, this could result in the facial scan of a casino patron who was not engaged in illegal activity, being temporarily retained in the OPP database until the investigation was concluded.

We accept that this temporary retention of personal information is a necessary part of the criminal investigation process. However, we believe that members of the public should be made aware of the fact that a biometric scan of their face could, in exceptional circumstances, be temporarily collected and retained upon entering a casino in Ontario. Such notice could be achieved by posting signs at all casinos notifying patrons that the OPP uses face recognition technology at Ontario casinos.

We also take the position that subsection 14(1)(c) would not exempt the institution from the requirement to provide a general notice to the public. During the course of our investigation, we were informed that professional casino cheats are fully aware of the fact that face recognition technology is being used in casinos, including those in Ontario. We accept that, at this point in time, not all casino patrons may be aware of the use of face recognition technology in casinos. But knowledge of its use is quickly growing in Ontario and can only become more widespread.

In addition, notice of the use of face recognition technology by the police may have a deterrent effect on "small-time cheaters." They may well decide not to risk engaging in criminal activity where such technology is used since it could pose an additional threat to their efforts at evading apprehension. In our view, the deterrent value of posting notice could only benefit law enforcement efforts at keeping Ontario casinos free from criminal activity.

The use of face recognition technology by law enforcement agencies has been widely reported in the media in both Canada and the U.S. Private-sector companies that supply face recognition technology to law enforcement agencies and casinos, including Biometrica Systems, Inc., openly advertise their products on the Internet and elsewhere. Consequently, although a general notice would provide information that this investigative technique is currently being used in Ontario

casinos, it could not, in our view, be said to “reveal” such a technique since this information is already in the public domain.

There are also strong policy reasons for requiring government institutions to provide public notice if they are surreptitiously using biometric technologies to capture personal information. Face recognition technology enables law enforcement agencies to collect an individual’s personal information covertly from a remote location without that individual’s specific knowledge or consent. Once scanned, an individual’s facial image can then be entered into a database and retained indefinitely if there are insufficient controls in place. Unlike simple surveillance by remote cameras, a facial scan can also be used to match an individual’s unique facial characteristics with a broad database of images.

We do not believe that individuals surrender complete control over their physical autonomy and personal information when they enter a casino. Consequently, unless a specific, probable harm can be identified, government institutions should be required to notify the public if face recognition technology is being used in a public location.

We note that many of the companies that supply biometric technology to law enforcement agencies support the principle of public notification. On February 2, 2001, the International Biometric Industry Association (IBIA) released a statement that reiterated its policy on the use of biometrics by government agencies. In particular, IBIA Executive Director Richard E. Norton noted, “Our companies recommend that clear signage or other means of notification be used to inform everyone that video imaging and facial recognition technology are being used in a public area.” We couldn’t agree more.

In our view, the AGCO should post signs at all casinos notifying patrons that the OPP may be collecting their personal information through the use of both video surveillance and face recognition technology.

Conclusion: The AGCO should provide proper notice, under section 39(2) of the *Act*, of the collection of personal information.

**Issue D: Is the OPP’s use of the personal information in compliance with section 41 of the *Act*?**

Section 41 of the *Act* sets out the circumstances under which an institution may use personal information. Subsection 41(b) states that an institution shall not use personal information in its custody and control except for the purpose for which it was obtained or compiled or for a consistent purpose.

OPP officers assigned to casinos obtain or compile personal information about suspects through the use of face recognition technology. If an officer has a reasonable suspicion that an individual is engaging in criminal activity, he or she can freeze the video feed and produce a still image of

the suspect's face. In our discussion of Issue B, we concluded that this personal information was being collected for the purposes of law enforcement.

The officer then puts the collected personal information to a specific use. As part of a law enforcement investigation, he or she attempts to identify the suspect by comparing the still image to databases of known and suspected criminals. In our view, this matching process takes place for the purpose of assisting officers with their law enforcement duties. In particular, it helps them to prevent gaming-related crimes, apprehend individuals who violate the *Criminal Code*, and lay charges against alleged cheaters.

The AGCO and OPP have assured us that the scans are not being used for purposes other than law enforcement. If an OPP investigation concludes that an individual was not involved in illegal activity, the scan is immediately deleted. If the investigation concludes that the person was engaged in illegal activity, the information is retained in the OPP database at that particular casino. Thus, the OPP is using the personal information under its custody and control only for the purposes for which it was obtained or compiled.

Conclusion: The OPP's use of the personal information is in compliance with section 41 of the *Act*.

## **OTHER MATTERS**

### **Consultation**

On numerous occasions, we have urged the Ontario government to consult with our office before launching any initiatives or programs that may impinge on privacy. We have also advocated the use of privacy impact assessments to examine the privacy implications of new initiatives. Neither the AGCO nor the OPP consulted with our office or conducted a privacy impact assessment before implementing the use of face recognition technology in Ontario casinos. The AGCO submits that it was not aware of any requirement to consult with our office. We accept that position. The AGCO also believes that a privacy impact assessment was not necessary because "the system is an investigative tool that is used by the OPP in a very specific environment." We accept that the face recognition system is an investigative tool used in narrow circumstances, nonetheless, we believe that a privacy impact assessment would have been useful.

The *Act* does not specifically compel institutions to consult with our office before launching initiatives or programs that may have privacy implications. However, section 59(a) of the *Act* gives the Commissioner the power to offer comment on the privacy protection implications of proposed legislative schemes or government programs. In addition, under section 59(b), the Commissioner may order an institution to cease existing collection practices or order the destruction of collections of personal information that contravene the *Act*.

We would suggest that consultation with our office is in accordance with the spirit and intent of the *Act*, but more so, can assist institutions in ensuring that they are in compliance with the *Act*.

It is particularly important for institutions to consult with our office before implementing any *biometric* programs or other technologies that may impinge on privacy.

As with many new technologies, biometric technologies and their potential uses are viewed with mistrust by some members of the public. The fear is that biometric systems could later be used without notification for additional, secondary purposes not intended when the original system was implemented. Technologies that serve to monitor the activities of individuals also lead to an increased feeling that there are fewer and fewer private spaces remaining in which people can feel free from surveillance.

The sophistication of biometric technologies is also rapidly expanding. As noted earlier in this report, the Tampa Police Department in Florida used video surveillance cameras and face recognition software in the week leading up to the 2001 Super Bowl. On the day of the game, the faces of an estimated 100,000 fans and workers who passed through the football stadium turnstiles were digitally scanned and compared to an extensive customized database of known felons, terrorists and con artists provided by local, state, and federal law enforcement agencies. The Super Bowl surveillance was heavily criticized by the ACLU, which called on the Tampa City Council to schedule public hearings on the matter. They feared that the growing use of these technologies could lead to a society under constant surveillance.

An additional form of face recognition technology is also being developed that would enable law enforcement agencies to photograph a large crowd of people and efficiently scan the faces of everyone in that crowd (commonly known as “face-in-a-crowd” detection). Our understanding is that this form of face recognition technology is still being tested and has yet to be made commercially available.

Our investigation found that the OPP is not scanning the face of every person entering into a casino, nor is the OPP considering doing so. However, it would not necessarily be far-fetched to suggest that law enforcement agencies in Ontario may, at some time in the future, be tempted (as they have elsewhere) to use such face recognition technology for criminal investigation purposes in other environments, such as at sporting events or other large public gatherings. We strongly advise against doing so and urge all government institutions, including law enforcement agencies, to consult with our office before launching any such initiative. The prospect of covert surveillance encroaching into more and more public spheres of activity poses a serious threat to our fundamental right to privacy.

## **SUMMARY OF CONCLUSIONS**

Our investigation has concluded that:

(A) The information collected by the OPP through the use of face recognition technology is “personal information” as defined in section 2(1) of the *Act*.

(B) The OPP's collection of personal information is in compliance with section 38(2) of the *Act*.

(C) The AGCO should provide proper notice, under section 39(2) of the *Act*, of the collection of personal information.

(D) The OPP's use of the personal information is in compliance with section 41 of the *Act*.

## RECOMMENDATIONS

(1) The AGCO should post signs at all commercial and charitable casinos to notify patrons that the OPP may be collecting their personal information through the use of both video surveillance and face recognition technology. We recognize that it may not be practical to list all of the information required by section 39(2) of the *Act* on a public sign. Consequently, we recommend that the AGCO also make materials publicly available at casinos that notify patrons that the OPP may be collecting their personal information through the use of both video surveillance and face recognition technology. In accordance with section 39(2) of the *Act*, these materials should set out the legal authority for the collection; the principal purpose or purposes for which the personal information is intended to be used; and the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

(2) The AGCO should consult with the Office of the Information and Privacy Commissioner before broadening the existing use of face recognition technology or employing new forms of biometric surveillance in Ontario casinos.

(3) All government institutions, including law enforcement agencies, should consult with the Office of the Information and Privacy Commissioner before launching any initiative or program that involves the use of biometric technology.

Within three months of receiving this report, the AGCO should provide the Office of the Information and Privacy Commissioner with proof of compliance with recommendation (1).

Original signed by:  
Ann Cavoukian, Ph.D.  
Commissioner

\_\_\_\_\_  
Date