INFORMATION AND PRIVACY COMMISSIONER OF ALBERTA

Report of an investigation on the use of a hand recognition system

August 7, 2008

Southwood Care Centre, Intercare Corporation

Investigation Report F2008-IR-001

(Investigation F4400)

Introduction

[1] On February 15, 2008, the Information and Privacy Commissioner received a complaint from an employee at the Southwood Care Centre nursing home in Calgary, objecting to the use of a hand scanner to clock in and out of work.

[2] The Commissioner authorized me to conduct an investigation under section 53(2)(e) of the *Freedom of Information and Protection of Privacy Act* (FOIP). Section 53(2)(e) allows the Commissioner to conduct investigations and resolve complaints that personal information has been collected, used or disclosed in contravention of Part 2 of FOIP, which addresses protection of privacy.

Background

[3] In her letter to our office, the complainant stated, "I'm concerned about my privacy since I don't think the company has a right to take my handprint and I don't think my information will be protected since the office is not locked during the day and the office staff does not require a password or swipe card to get in and out of the office. I am very concerned about this practice and I would prefer not to clock in and out of work in this manner… The company has not explained anything to its staff about this practice and is basically forcing its employees to comply with this practice."

[4] Southwood Care Centre is a long term care centre located in south east Calgary. It provides the following services: general long term care, specialty care for brain injuries, dementia and Alzheimer's disease and hospice care. The Southwood Care Centre is one of four long term care centres in Calgary run by Intercare Corporation. Intercare's Head Office is located in Vancouver, British Columbia.

[5] The hand recognition system consists of a hand scanning device at each Intercare location with network connections to Intercare's payroll system. When employees report for work, they place one hand on the scanner to verify their arrival time. They also enter an employee identification number. Employees repeat the same process at the end of their shift. A hand scanning device has been installed at each Intercare nursing home.

[6] The hand scanning device (or hand scanner) is a small terminal (approximately 22cm wide, 30cm high and 22cm deep), attached to the wall at about waist height. It has a flat surface on which the user places his or her hand. A numeric key pad allows users to input numbers. A small screen provides feedback to the user, indicating whether a hand scan has been successfully recognized or not. The screen also displays administrative functions, used to register and de-register employees.

[7] Intercare uses an Ingersoll Rand Schlange HandPunch 3000 hand scanner. According Ingersoll Rand's website, the device works as follows:

> The HandPunch measures the unique size and shape of the fingers and hand. Over 90 different measurements are made such as, length, width, thickness and surface area. No finger prints or palm prints are taken.
> …
> To enroll an employee for the first time, the employee would put their hand into the HandPunch three times so that a CCD camera records 3 images of the hand. An algorithm converts these images into one mathematical value (Your template). This template is then stored in the HandPunch. Each time an employee puts their hand in the HandPunch to punch in or out of work, the HandPunch takes another image of the hand, the algorithm converts this image to a mathematical value and then compares this new template with the template the HandPunch has stored previously. If the two templates match, identity is confirmed and the punch is recorded.
> …
> Hand geometry units do not store the image of the hand, but instead store a 9-byte template which is a mathematical representation of the hand image. This mathematical value is meaningless to other devices. In addition, no fingerprint or palm print information is gathered.[1]

(The abbreviation CCD above means "charge-coupled device" and in this context refers to a kind of image sensor, also commonly used in digital photography.)

[8] The mathematical value mentioned above (i.e. the template) is associated with the identification number the employee enters when using the hand scanner. Time and attendance data verified by the hand scanner are sent to the payroll system for processing. Data from the hand recognition system are linked to the payroll system using the employee identification number.

[9] The hand recognition system as described is an authentication system. Authentication systems confirm the identity of a person by comparing something the person provides with information that was previously provided by or assigned to the

[1] http://recognitionsystems.ingersollrand.com/faq, viewed July 15, 2008

same person. In this case, employees register themselves in the system by having their hands scanned, which generates a unique number (the "template"). Whenever an employee clocks in or clocks out, they put their hand on the scanner and it rescans their hand. If the template generated at this point matches the template and code number previously registered in the database, the employee's identity is verified. Therefore, information is collected at the time of registration, and again each time the employee places their hand on the scanner to clock in or clock out.

[10] At the time of publication of this report, the system was not fully implemented. Employees were registered in the hand scanning system, but had not begun using it to clock in and out of work. Full implementation is planned for September 2008.

Application of FOIP

[11] Intercare Corporation is the operator of a nursing home (Southwood Care Centre) as defined in the *Nursing Homes Act*. Therefore, Intercare falls under the definition of "health care body" set out in section 1(g)(ii) of FOIP, making it a "public body" under section 1(p) of the FOIP.

[12] The complainant provides services to Intercare in a contract or agency relationship and is therefore considered an "employee." as defined in section 1(e) of FOIP.

[13] As an operator of a nursing home under the *Nursing Homes Act*, Intercare is also a "custodian" under the *Health Information Act* (HIA). The complainant, as an employee of a custodian, could also be considered an "affiliate" and a "health services provider" under the HIA. The HIA applies to health information collected, used and disclosed in the provision of health services. While health services are provided at Southwood, the information in question here is collected in a different context. The hand recognition system is not used in the provision of any health service; rather it is used to track hours worked for management purposes. Therefore, the HIA does not apply to this situation.

Issues

[14] Is the information collected by the hand recognition system personal information under the *Freedom of Information and Protection of Privacy Act*?

[15] Did the pubic body collect, use or disclose personal information in contravention of Part 2 of the *Freedom of Information and Protection of Privacy Act*?

Findings

Is the information collected by the hand recognition system personal information?

[16] FOIP defines personal information in section 1(n). The two categories of personal information pertinent to this question are included in subsections iv and v as follows:

> (n) "personal information" means recorded information about an identifiable individual, including
>
> …
>
> (iv) an identifying number, symbol or other particular assigned to the individual,
>
> (v) the individual's fingerprints, other biometric information, blood type, genetic information or inheritable characteristics,

[17] While the hand scanner does not record a hand print, as suggested by the complainant, it does collect measurements of an employee's hand, from which it generates and records a unique number. The unique number generated from the hand measurements is an identifying number assigned to an individual and is included in the definition of personal information in FOIP section 1(n)(iv). The identification numbers employees enter when using the hand scanner also fall under this definition.

[18] Section 1(b.1) of FOIP defines "biometric information" as "information derived from an individual's unique measureable characteristics." Hand measurements are a measurement of an individual's physical characteristics and are used here as a way to uniquely identify individuals. In my opinion, hand measurements are biometric information as set out in section 1(n)(v) of FOIP.

[19] To be considered personal information for the purposes of FOIP, the information must also be recorded. While the scanning device does not store hand measurements in its memory, it must record them for at least the amount of time necessary to allow the scanner's processor to calculate the template, both at registration and later, as employees clock in and out. FOIP does not state how long information must be stored to be considered "recorded." In my opinion, the hand print information is recorded. Therefore, I find that hand measurements are "biometric information" and fall within the definition of "personal information" set out in FOIP.

[20] Both the hand measurements and the numbers derived from these measurements are personal information under FOIP.

Did Intercare collect, use or disclose personal information in contravention of FOIP?

[21] While the system has not been fully deployed, employees have been registered in the hand recognition system. Intercare has collected their personal information.

[22] The complainant questioned whether Intercare had a right to collect her handprint, stated that she had not been informed about the practice and expressed concern that her information may not be secure. In addressing the complainant's concerns, I will consider the following sections of Part 2 of FOIP:

a. Section 33(c) of FOIP places a duty on public bodies to only collect personal information that relates directly to and is necessary for an operating program or activity of the public body.

b. Section 34(2) of FOIP states that the public body must inform the individual from whom information is being collected of:

i. the purpose for which the information is collected
ii. the specific legal authority for the collection, and
iii. the title, business address and business telephone number of an officer or employee of the public body who can answer the individual's questions about the collection.

c. Section 38 of FOIP says that the public body must protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction.

Collection of personal information

[23] Pursuant to FOIP section 33(c), I will consider whether the collection of personal information through the hand recognition system relates directly to an operating program or activity of Intercare and whether this collection is necessary.

[24] Intercare advised me that it was implementing the hand scanner for the following purpose:

> The system is used as the means to identify the employee who is logging in and logging out from their assigned shift such that their attendance can be recorded accurately in the payroll system and the employee compensated accordingly for the hours of work.

[25] In order to operate its programs and services, Intercare needs to compensate its employees. Employee compensation is necessary to support virtually all operating activities of a nursing home. Accurate data are needed to calculate hours worked and pay employees accordingly. In my opinion, gathering information that uniquely identifies employees and tracks their working hours is directly related to employee compensation and supports an operating activity of the public body.

[26] In determining whether this collection of personal information is necessary, a review of Commissioner's Order F2005-003 is instructive. In this Order, the Commissioner found that collecting personal information about an employee through keystroke-logging software was not necessary to manage his performance in the circumstances. The Commissioner agreed that gathering information to manage an employee may fall within section 33(c), but determined that gathering this information through keystroke logging software was not necessary because:

a. There was insufficient evidence to support the library's concerns that the employee needed to be monitored.
b. By collecting information on everything the employee did on his computer, the public body collected too much personal information.
c. The keystroke logging software was installed on the employee's computer surreptitiously, making it an intrusive way of collecting information.

At paragraph 30 of his Order, the Commissioner stated, "In my view, information collected by keystroke logging software becomes 'necessary' within the meaning of section 33(c) of the *Act* only when there is no less intrusive way of collecting sufficient information to address a particular management issue."

[27] While the facts of this investigation are quite different, the question of necessity is similar. I have agreed that gathering accurate data on the hours employees work is directly related to operating the nursing home, but I also need to consider whether collecting this information through a hand recognition system is necessary. Following Order F2005-003, I will base my finding on the following three considerations:

a. Is there evidence to indicate the hand recognition system responds to a management concern and that alternative systems do not?
b. By using a biometric authentication system, is Intercare collecting too much personal information to support employee compensation?
c. Is the biometric system intrusive?

Does the hand recognition system respond to a management concern?

[28] A biometric authentication system is not the only option available to authenticate employees as they clock in and out of work. There are a number of methods to verify a person's identity. There are generally three things, known as "factors of authentication," people can provide to confirm their identity:

a. Something they know (e.g. a password)
b. Something they have (e.g. an identity card)
c. Something they are, or do (e.g. biometric information)

[29] I asked Intercare whether it had considered other factors of authentication to meet their stated purpose of identifying employees and compensating them appropriately. Intercare is currently using a magnetic card system, where employees clock in and out by swiping their cards through a card reader and providing a 4 digit code. This system was rejected for the following reasons:

a. inability to know whether the employee swiping the card is indeed the employee who has been assigned that card
b. employees regularly forget, lose or damage swipe cards, resulting in a need for employees to fill out a "swipe card discrepancy form," which in-turn needed to be signed by their supervisor, causing administrative burden
c. delays in registering new employees with swipe cards, caused by lack of card inventory and waiting for payroll staff to program the cards.

[30] When an employee clocks into a payroll system using another person's card, this is commonly known as 'buddy punching' and is related to reason a. above. I asked Intercare whether they had experienced any instances of buddy punching with their card reader system. Intercare stated that it had dismissed one employee for buddy punching on behalf of one of her colleagues and that buddy punching remained an ongoing concern. Reasons b. and c. above also point to administrative burden related to the card reader system. With the hand recognition system, employees cannot forget their hands at home and there is no need to wait for payroll staff to program cards.

[31] Other alternatives, such as having a manager supervise staff as they sign in and sign out in a log book, for example, do not seem practical in a long term care facility with workers coming and going at all hours and would result in additional expense.

[32] I believe there is evidence to support Intercare's claim that alternative authentication systems would not meet its business needs and that the hand recognition system responds to a management concern.

Is too much information collected?

[33] The hand scanner device collects hand measurements from employees and employees enter an identification number. If the number derived from these measurements and the employee number match, the scanner assigns the current time to the employee's arrival or departure. The hand scanner is therefore collecting the time the employee arrived for work, the time the employee ended their shift, and authentication information to uniquely identify the employee. In my opinion, this is the minimum amount of information needed to support the accurate calculation of hours worked. Intercare is not collecting too much employee information through its hand recognition system to support employee compensation.

Is the hand recognition system intrusive?

[34] In describing the keystroke logging system in Order F2005-03 the Commissioner pointed out that the system was surreptitious, making it "intrusive." In examining its intrusiveness, I will consider whether the hand recognition system is surreptitious, as well as two other factors I believe relevant to this investigation: whether participation is mandatory and whether the information gathered would be useful in any other context. These points were not relevant in Order F2005-003, but I believe they need to be considered in this investigation, given the concerns expressed by the complainant.

[35] A system that attempted to gather biometric information without the knowledge of those affected would very likely be considered intrusive. However, Intercare's hand recognition system does not gather personal information surreptitiously. In order for the system to work, employees need to register. At this point, and when they clock in and out of work, it would be obvious to employees that a hand scanner was in use. (I will discuss the notice Intercare gave to its employees about the system later in this report.)

[36] The complainant stated that Intercare was "forcing" employees to use the hand recognition system. Intercare confirms that using the system will be mandatory, as they will be phasing out the card reader system, along with an older payroll system. The new payroll system is not compatible with the old card reader system. In my opinion, making the use of the system mandatory increases its intrusiveness.

[37] The complainant was under the impression that the hand scanner would "take [her] hand print." If the hand recognition system gathered biometric information that was useful in another context, this would represent a potential privacy risk. For example, if the hand scanner captured an image of the employees' palms or fingerprints, this information could be used in a law enforcement context. Having employees participate in a mandatory system that increases risk to their privacy would certainly be intrusive. However, the system does not gather a palm print or finger print; it collects hand measurements, which it translates into a unique number (the template). The template is useful only when combined with the employee's identification number and the payroll system at Intercare. It seems unlikely that the template could be put to any other use, mitigating the privacy risk and making it less intrusive.

[38] There is evidence to indicate the hand recognition system responds to a management concern and that Intercare considered and tried other options that did not meet its business needs. The hand scanning system is mandatory, making it somewhat intrusive. At the same time, it does not gather more information than needed, it does not gather information surreptitiously, and the personal information gathered would not likely be useful in any other context. In contrast to the circumstances described in Order F2005-003, Intercare has provided more evidence that the system meets a management need. Furthermore, the hand recognition system is less intrusive than the keystroke logging system. On balance, I find that the information gathered by the hand recognition system is necessary to support an operating program or activity of the public body. Therefore, I find the public body has not collected personal information in contravention of section 33(c) of the *Freedom of Information and Protection of Privacy Act*.

Notice

[39] I asked Intercare whether it had given any notice or explanation to employees about the hand scanning system. The new system was first announced in the Intercare employee newsletter, "Intercare Connection" in February 2007. The article reads as follows:

> New Payroll Program
> Intercare is currently in the process of transferring to a new payroll program and provider. You may notice new hand readers next to the current swipe card machines at your respective facilities. This highly effective and efficient system will replace the swipe card machines and will provide our employees with a mechanism where they do not have to worry about remembering to bring their swipe card into work. All you will need is your hand! Please continue to use the current swipe card machine and do not attempt to use the hand readers until further notice. Our hope is to have our new payroll system up and running by April 1st, 2007. We will keep our staff updated on the progress being made.

[40] A second article appeared in "Intercare Connection" in the April 2008 edition:

> Employee Hand Readers For Payroll
> As Intercare moves closer to going live with its new payroll program, our Leadership team has worked extremely hard to get their staff setup on the biometric hand readers which will assist us in accurately processing the payroll. We would like to remind and ensure all staff that in no way does this hand reader system pose a risk to your personal identity or provide the ability for anyone to illegally obtain information pertaining to your identity. The hand reader system does not read the markings on your hand so therefore, in no way could someone use the information provided for anything other than our payroll program. It will be mandatory for all employees to be enrolled on this system once we do go live. Should there be any concerns, please contact [employee name] at [phone number] for further information.

[41] The above articles go some way toward explaining the hand recognition system. From my reading of the articles, the purpose of the system is clear. Also, the second article provides contact information for a person who can provide further details and answer questions.

[42] While the newsletter articles represent a good start, they do not fulfill all of the requirements of section 34(2) of FOIP. The articles do not cite the specific legal authority under which the personal information is collected, as required by section 34(2)(b) of FOIP. Proper notice must include all three elements set out in FOIP section 34(2)(a), (b), and (c). This requirement was confirmed in this Office's Investigation Report 2000-IR-004.

[43] Further, it is not clear that all those whose information was collected would have seen the articles. For instance, the complainant says she did not notice these articles. Ideally, notice should be provided at the time of collection so it is obvious to the individual why their information is being collected. This best practice is supported in this Office's Investigation Report 2000-IR-007 where the Commissioner found that a school should have provided students or parents with a collection notice at the time school photographs were taken, rather than earlier, at school registration. Therefore, the best options Intercare could have exercised were:

a. to provide proper notice at the time employees were initially registered in the hand recognition system, and/or,
b. to provide proper notice on a poster near the hand scanner that would be seen each time employees clocked in and out.

[44] Therefore, because Intercare did not provide a proper collection notice, I find that the public body did not meet the requirements of section 34(2) of *Freedom of Information and Protection of Privacy Act*.

Protection of personal information

[45] The complainant expressed concern that her personal information collected through the hand recognition system would not be safe. To address this concern, I examined whether Intercare met its obligations under section 38 of FOIP to make reasonable security arrangements to protect personal information.

[46] In particular, the complainant raised a concern that the Southwood facility administration office was not locked during the day and that staff did not use security cards or other means to gain entry. I visited this office, located on the ground floor of the facility. Access to the payroll system and some administrative functions of the hand recognition system would be accessible through computers in the office, but these applications are protected by strong passwords that use a combination of letters, numbers and symbols. Staff at Intercare must display photo identification badges and visitors are accompanied at all times. Finally, entrance to the office is controlled by a receptionist. Reasonable security measures are in place in Intercare's administrative office to protect computer terminals with access to the hand recognition system.

[47] Hand measurements are transformed by way of a mathematical formula, or algorithm, into a 9 byte block of data ("the template," as described in paragraph 7). This formula works in one direction: inputting hand measurements into the formula results in a unique template. Going in the other direction, it would be difficult to derive a person's hand measurements from the template. While it may be possible to reverse engineer the template, it would require access to data in the system and an advanced knowledge of mathematics.

[48] I inspected the hand scanning device, located in the lobby of the Southwood facility. The device is securely attached to the wall, with no exposed wires that could be tapped. The device is in a busy, public area of the facility, where it is likely that anyone tampering with it would be noticed.

[49] Supervisors have the authority to add and remove employees from the system at the hand scanning device. Supervisors authenticate to the system by scanning their hands and entering a supervisor code.

[50] No data is stored in the hand scanning device itself. All hand scanning data is held in a database, housed on a network server at the Southwood site. All payroll data is transmitted and stored in encrypted format. I inspected the network server room. The room is kept locked and the server is installed in a locked metal cage. Only the system administrators have access to the server room.

[51] The server is protected by strong passwords, a firewall and anti-virus service. The server's operating system, firewall and antivirus service are patched and updated regularly. Server data are backed up daily and data recovery is tested regularly.

[52] In my opinion, the public body has made reasonable security arrangements to protect personal information against such risks as unauthorized access, collection, use and destruction, as required by section 38 of FOIP.

Recommendations

[53] I recommended that Intercare post a collection notice that meets the requirements of FOIP section 34(2) at each hand scanner at each of its sites. Intercare has agreed to carry out my recommendation when it fully implements the hand scanning system (implementation projected for September 2008).

[54] I further recommended that Intercare provide notice to all new employees who will be registered in the hand scanning system, at the time of registration. Intercare agreed to carry out this recommendation immediately.

Conclusion

[55] This case illustrates the need for public bodies to provide a proper collection notice when implementing new information systems. In this case, I found that the public body's use of a biometric authentication system was necessary. This finding does not represent a "privacy carte blanche" for public bodies to implement biometric systems. Public bodies need to demonstrate their use of these systems is necessary under the *Freedom of Information and Protection of Privacy Act*.

[56] I would like to thank Intercare for its openness and cooperation throughout this investigation.

Brian Hamilton, CISA
Portfolio Officer
Office of the Information and Privacy Commissioner of Alberta