Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

INVESTIGATION REPORT P17-01

Use of employee surveillance by a BC chicken catching organization

November 8, 2017

Drew McArthur
Acting Information and Privacy Commissioner for British Columbia

November 8 2017

CanLII Cite: 2017 BCIPC 58
Quicklaw Cite: [2017] B.C.I.P.C.D. No. 58

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

In June 2017, a covert video depicting disturbing images of animal abuse at a chicken farm was released to the media. Animal rights groups and British Columbians alike immediately condemned the actions of some employees of the Lower Mainland "chicken catching" company. Acting on the advice of a crisis management consultant, the company decided to require their crews to wear surveillance video cameras as they worked.

My office unequivocally condemns all forms of animal abuse. But after reviewing the media coverage of this matter, I was concerned that video surveillance was being used as a "quick fix," without thoughtful consideration of its potential privacy impacts. For this reason, I decided to investigate whether the company's use of video surveillance was compliant with British Columbia's *Personal Information Protection Act* (PIPA).

Through interviews with the company, my investigators learned that it had two goals with its video surveillance: to prevent future instances of employee misconduct and to restore the company's reputation. But video surveillance should only be used as a last resort, not as a substitute for ineffective recruitment and training protocols.

The company did not assess the privacy risks associated with implementing video surveillance. In addition, the employees subjected to the surveillance were not the same employees who were responsible for the misconduct; those individuals no longer work for the company.

We found that the company was not authorized to collect the information under PIPA because the purposes for which it was collecting and using personal information were not reasonable. The company was also collecting personal information without consent from other individuals, including farmers, truckers, and contractors.

Video surveillance, as we all know, has become pervasive in our society. Too often, organizations like this one turn to surveillance believing it will fix their crisis or problem. Organizations need to understand the privacy risks associated with surveillance and take all reasonable efforts to avoid them.

ORIGINAL SIGNED BY

Drew McArthur
A/Information and Privacy Commissioner
for British Columbia

EXECUTIVE SUMMARY

The Acting Information and Privacy Commissioner initiated this investigation after learning that a chicken catching organization (the Company) was using audio and video surveillance (surveillance) to monitor its employees. Under the authority of section 36(1)(a) of the *Personal Information Protection Act* (PIPA), the Office of the Information and Privacy Commissioner for BC (OIPC) investigated the Company's use of a body worn surveillance system.

The issues addressed in this investigation report are:

1. Does the Company collect "personal information" as defined by s. 1 of PIPA?
2. Does the Company collect "employee personal information" as defined by s. 1 of PIPA?
3. Does PIPA authorize the Company to collect and use that information?
4. Has the Company complied with its PIPA obligations regarding policies and practices?

The investigative methodology included an analysis of the Company's policies, practices and employee training; a site visit; interviews with key Company executives; examination of the surveillance system; and review of surveillance samples.

The assessment criteria for this investigation included the responsibilities of the organization under PIPA, OIPC guidance documents, and OIPC orders.

The key findings resulting from this investigation are:

1. The Company is collecting personal information when it collects audio and video surveillance recordings of individuals as they work on private chicken farms.
2. The information that the Company collected by surveillance in this case does not constitute "employee personal information" under PIPA because the surveillance is not being collected "solely" for that purpose.
3. PIPA does not authorize the Company to collect the personal information of employees, farmers and other contractors via body worn surveillance devices. This is because it did not have consent and it was not authorized under PIPA to collect without consent. Moreover, a reasonable person would not consider the purposes for the collection to be appropriate in the circumstances. For example, there is insufficient evidence of a safety, security or employee management problem, nor evidence of other significant issues that would authorize the Company to monitor and video record employees, farmers and other contractors going about their duties. In addition, the Company failed to consider whether less privacy invasive measures were available for their purposes, and the surveillance was unlikely to be effective for the purpose of defending the company's reputation.

4. The company does not have any privacy policies in place that state the purpose for surveillance. It did not notify its employees and non-employees subject to surveillance that it would be collecting their personal information. Finally, it did not conduct a privacy impact assessment.

The Acting Commissioner made seven recommendations to the Company, including:

a) Ceasing any further video and audio collection of surveillance information and deleting all stored recordings of personal information collected via surveillance;

b) Conducting a privacy impact assessment prior to introducing any other privacy invasive technology system in the future; and

c) Creating the necessary privacy policies and procedures to ensure the Company complies with PIPA.

1.0 INTRODUCTION

This investigation report examines a chicken catching organization (the Company) that used a body worn audio and video surveillance (surveillance) system to monitor its employees. The Company offers chicken catching services to both farmers and large poultry processing companies located in British Columbia.

The Company implemented surveillance in response to several media stories that alleged Company employees had abused chickens. Upon reviewing the media stories, the Acting Information and Privacy Commissioner decided to investigate the Company's use of surveillance.

The purpose of this investigation is to determine whether the Company's surveillance system is compliant with the *Personal Information Protection Act* (PIPA) and whether the Company had appropriate privacy policies in place. The report makes seven recommendations to bring the Company into compliance with PIPA regarding the collection, use and/or disclosure of personal information.

1.1 Background

The Company, when under contract with either private chicken farms or chicken processing plants, sends a crew of up to fourteen employees, including one supervisor, to farms to catch chickens for safe transport to a processing plant.

In June 2017, covertly recorded videos that appeared to show some Company employees mistreating chickens became public. After these videos were released, some of the Company's

employees received death threats. In response, the Company hired a crisis management consultant to help manage the situation and restore its reputation.

The crisis management consultant recommended the Company video-record its employees to deter mistreatment of chickens and to restore customer confidence by showing that its staff handle chickens properly. The Company also wanted to demonstrate it has zero tolerance for animal abuse and that it was taking action to prevent future recurrence.

The Company implemented body-worn surveillance cameras, believing that if the employees knew they were being observed, they would be less likely to abuse the chickens. The Company did not consider any other method to inform or manage its employees to ensure that proper chicken handling practices in the Company's Standard Operating Procedures (SOP) were followed.

The Company employees subjected to the surveillance were not the same employees responsible for the prior misconduct, who no longer work for the company.

During the system testing phase, the Company discovered that the surveillance footage was poor quality due to low light levels, high volume squawking in the chicken barns, and the jerky recording from wearing body-cams.

One Company executive was responsible for viewing the surveillance from each shift to see whether any chickens suffered improper handling. During the initial testing phase of approximately one month, this Company executive did not note any misconduct in the surveillance recordings.

1.2 Investigative Process

Upon learning that the Company intended to use surveillance on its employees, the Office of the Information and Privacy Commissioner (OIPC) initiated an investigation to examine whether the Company's proposed surveillance system complied with PIPA.

As part of this investigation, an OIPC investigator interviewed two Company executives at their head office. These interviews explored the following issues:

a) The collection, use and disclosure of personal information contained in the surveillance system;

b) Description and capabilities of the surveillance system;

c) Storage of the surveillance;

d) Company policies and procedures relating to privacy and a surveillance system;

e) Company's privacy training for employees; and

f) Effectiveness of the surveillance footage.

The assessment criteria for this investigation are the requirements under PIPA and guidance materials from OIPC guidance document *Getting Accountability Right with a Privacy Management Program* dated April 17, 2012.

The investigator reviewed the Company's Standard Operating Procedures (SOP) and surveillance of the Company's employees.

The OIPC also provided the Company with an opportunity to discuss the proposed findings and recommendations prior to the Company submitting its response to the final draft of the investigative report.

2.0 PERSONAL INFORMATION PROTECTION ACT

PIPA governs the collection, use and disclosure of personal information by organizations in a manner that recognizes both the right of individuals to protect their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

PIPA defines an organization as "… a person, an unincorporated association, a trade union, a trust or a not for profit organization…". Under the *Interpretation Act* a "person" includes a corporation. Therefore, the Company is an organization and is subject to the provisions set out in PIPA.

Pursuant to PIPA, organizations must have the authority to collect, use and disclose personal information and are responsible for the personal information they collect. They must designate someone within the organization who is responsible for ensuring compliance with the legislative requirements.

3.0 ISSUES

Section 36(1)(a) of PIPA establishes the OIPC's statutory mandate and power to investigate an organization's compliance with PIPA.

The Company's surveillance recorded not only its employees but contractors and customers. The issues the investigator considered, as they relate to the information the Company collected, are:

1) Does the Company collect, through surveillance, "personal information" as defined by s. 1 of PIPA?

2) Does the Company collect, through surveillance, "employee personal information" as defined by s. 1 of PIPA?

3) Does PIPA authorize the Company to collect, use and disclose that information?

4) Has the Company complied with its PIPA obligations regarding policies and practices?

4.0 ANALYSIS, FINDINGS, AND RECOMMENDATIONS

Issue 1 – Does the Company collect, through surveillance, "personal information" as defined by PIPA?

PIPA defines "personal information" as "…information about an identifiable individual and includes employee personal information but does not include (a) contact information, or (b) work product information."

The OIPC previously determined that video capture of an individual amounts to the collection of that individual's personal information.[1] This includes surveillance of an individual while they are working.

Consequently, the Company is collecting personal information when it collects surveillance recordings of individuals as they work on private chicken farms.

Issue 2 – Does the Company collect, through surveillance, "employee personal information" as defined by PIPA?

PIPA defines "employee personal information" in s. 1 of PIPA as "… personal information about an individual that is collected, used or disclosed solely for the purposes reasonably required to establish, manage or terminate an employment relationship between the organization and that individual, but does not include personal information that is not about an individual's employment."

As noted in Order P12-01, the definition of "employee personal information" contains two elements.[2] First the collection, use or disclosure of information must be for "purposes reasonably required" to establish, manage or terminate an employment relationship. Second, the collection, use or disclosure must be "solely" for those purposes.

I will address the second element first. Regarding the second element, Commissioner Loukidelis stated:

[1] See for example, 2009 BCIPC 67292 (CanLII), para. 60.
[2] 2012 BCIPC No. 25 (CanLII), para. 116.

> …to be employee personal information, the personal information must be collected, used or disclosed "solely" for the purposes reasonably required to establish, manage or terminate the employment relationship. An employer cannot have a collateral purpose for collecting, using or disclosing the personal information and still claim the personal information is "employee personal information". For example, it is doubtful that an employer could claim that name and address information of individuals it hires is employee personal information when the organization collects it for the purpose of establishing the employment relationship and also for marketing products to employees. The marketing purpose taints the exercise and the employer must otherwise be on side with PIPA as regards its marketing use of the information.
>
> In this case, I find that it is only necessary for me to analyze the second element and I need not address the first element.[3]

As noted above, the Company advised the investigator that the purpose of the surveillance was to deter misconduct by its employees and to restore the Company's reputation by showing that chickens are handled properly.

Deterring misconduct by employees likely constitutes managing an employment relationship. However, the Company was also using surveillance for the additional purpose of restoring the Company's reputation. Therefore, the Company was not collecting the information "solely" for the purposes of managing its employees.

Therefore, the information collected by surveillance in this case does not constitute "employee personal information" under PIPA because the surveillance is not being collected "solely" for that purpose.

As the information collected by surveillance in this case does not constitute "employee personal information," this report does not analyze the applicability of ss. 13, 16 and 19 of PIPA, which govern the collection, use and disclosure of employee personal information.

The surveillance recordings of individuals not employed by the Company (e.g.: farmers and contractors) also does not include "employee personal information" as these individuals are not employees of the Company. Nevertheless, such recordings include the "personal information" of those individuals and the authority to collect, use, or disclose it is addressed in the next section.

As a result, there is no need to address the first element, which is whether the collection, use or disclosure of information was for "purposes reasonably required" to establish, manage or terminate an employment relationship.

However, even if the information captured by the surveillance in this case was solely for the purpose of deterring improper conduct of the employees (as recommended by the crisis

[3] 2006 BCIPC 37938 (CanLII), para. 48.

management consultant), I have doubts that such collection would be "reasonable." As former Commissioner Denham stated in Order P12-01, ss. 13 and 16:

> …refer to what is "reasonable for the purposes of establishing, managing or terminating an employment relationship between the organization and the individual". This requires a further determination, of whether the collection, use or disclosure of the employee personal information itself, not the purpose for it, is "reasonable". Sections 13, 16 and 19 are not redundant – they clearly contemplate further scrutiny, by applying to the collection, use, or disclosure an objective standard of what is reasonable, viewed in light of what a reasonable person would consider appropriate in the circumstances…[4]

PIPA limits the collection of personal of information by any organization by requiring that collection be for the purposes that a reasonable person would consider appropriate in the circumstances, even where it otherwise permits the collection.[5]

Order P09-02 determined that, with respect to video surveillance, the reasonable person standard requires that surveillance only be used as a last resort after less privacy invasive measures to achieve the business purposes have been exhausted.[6] It is difficult to see how the Company could meet this requirement in the absence of trying less privacy-invasive alternatives prior to implementing surveillance.

Issue 3 – Is the Company authorized to collect and use that personal information?

The OIPC's *A Guide to PIPA for businesses and organizations* provides basic principles for organizations to consider when determining how personal information is collected, used and disclosed:

a) Limit the collection of personal information to that which is necessary for the purposes you identify;

b) Only collect, use or disclose personal information if it is reasonable in regards to the sensitivity of the personal information in the circumstances;

c) Do not require someone to consent to the collection, use or disclosure of personal information beyond what is necessary to provide him or her with a product or service; and

d) Collect personal information by fair and lawful means.[7]

[4] 2012 BCIPC No. 25 (CanLII), para. 141.
[5] Section 11.
[6] 2009 BCIPC 67292 (CanLII).
[7] OIPC, April 10, 2012, at 9: www.oipc.bc.ca.

PIPA requirements for collection of personal information

PIPA contains two requirements that an organization must meet before it may collect personal information, pursuant to ss. 10(1) and 11.[8] One is that the organization must be authorized under PIPA to collect the personal information, whether with consent or without consent.[9] Another is that a reasonable person would consider the purpose for collection to be appropriate in the circumstances.[10]

Requirement 1: Authority to collect personal information

Collection of personal information with consent

Section 6 of PIPA prohibits organizations from collecting, using or disclosing personal information about an individual without their consent, except in limited circumstances. A key component of consent is that the individuals whose personal information will be collected are aware of the purposes for collecting it.[11]

Pursuant to s. 10(1)(a) of PIPA, to obtain consent for the collection of an individual's personal information, an organization must provide the individual with notification of the purposes for the collection. Notification may be verbal or written, and must be sufficiently detailed for the individual to understand the purpose for the collection of their personal information. PIPA only considers consent to be valid if the individual is informed of the purpose for which their personal information will be collected.

At a group meeting, the Company told its employees that the surveillance was a preventive measure to protect the employees' reputations. This was the only purpose for the collection of the surveillance information that the Company communicated to its employees.

The Company also believed that the surveillance recordings, if it demonstrated proper handling of the chickens, could be used to refute any future allegations of animal abuse.

However, the Company did not explicitly inform employees that the surveillance could be used for managing their employee relationship with the Company and that the Company could discipline the employees if the surveillance recordings showed that they were not following the SOP.

The Company also did not tell its employees that it might show the surveillance recordings to its customers to manage the Company's reputation.

[8] For further discussion, see *Audit & Compliance Report P16-01,* 2016 BCIPC 56.
[9] See ss. 6-8 and ss. 12-13.
[10] See section 11.
[11] Section 10 of PIPA.

Employees did not sign a consent form to confirm that they were aware of the Company's intended uses for the surveillance.

The Company also did not notify non-employees that might have been subject to the surveillance, nor obtain their consent.

The Company instructed its supervisors to turn the surveillance on at the beginning of a shift, when they entered a chicken barn and to turn it off when they left the barn. However, if the truck drivers, farmers or other contractors entered the barn or the supervisor forgot to turn the surveillance off when exiting a barn, then their images and voices would be captured as well.

The Company owner acknowledged that any individual entering a barn while surveillance was in progress would not receive notice of the surveillance. The Company did not seek the consent of anyone on the farm prior to collecting their personal information via surveillance.

None of the farmers or contractors received notice that they were subject to surveillance. The Company did not advise them of the purposes of the surveillance and it did not post notification signs to alert individuals that they were entering an area where surveillance was being conducted. Consequently, the Company did not obtain the consent of each individual whose image was captured via surveillance.

Therefore, the Company did not clearly communicate the purposes for which the video surveillance would be used, and it did not obtain the informed consent of the individuals subject to the surveillance.

Implicit consent

Pursuant to s. 8 of PIPA, an individual is deemed to have consented to the collection of personal information if, at the time consent is deemed to have been given, the purpose for collection would be considered obvious to a reasonable person and the individual voluntarily provides their personal information to the organization for that purpose.

In this case, the purposes for the surveillance were neither clearly communicated to the Company's employees or non-employees subject to surveillance, nor sufficiently obvious to provide for deemed consent.

In addition, the Company did not give its employees or non-employees subject to surveillance an option to refuse consent as s. 8 of PIPA requires. The Company took the position that, if an employee objected to the use of surveillance, they could refuse to continue to work for the Company. None of the current employees refused to work while being under surveillance.

Consequently, I find that the Company did not provide sufficient notice to its employees or to non-employees subject to surveillance to meet the requirements for deemed consent under s. 8(1) of PIPA.

As the Company did not have consent of its employees or non-employees subject to surveillance, it was not authorized to collect their personal information via surveillance on that basis.

Collection without consent

PIPA authorizes the collection of personal information without consent in certain circumstances. For example, s. 12(1) of PIPA allows for collection without consent for various reasons, including:

- the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;
- the collection is necessary for the medical treatment of the individual and the individual is unable to give consent; or
- it is reasonable to expect that the collection with the consent of the individual would compromise the availability or the accuracy of the personal information and the collection is reasonable for an investigation or a proceeding.

The Company did not suggest that it was collecting the personal information of its employees or non-employees for any of the purposes outlined in s. 12(1) of PIPA. Nor did the OIPC find that any of these circumstances apply to the Company's collection of personal information via surveillance.

Therefore, I find that the Company had no authority to collect the personal information of these individuals without consent as contemplated by s. 12(1).

Requirement 2: Would a reasonable person consider the collection to be appropriate?

Sections 11 and 14 set out PIPA's reasonable person test.

Whether or not an organization obtained consent for collection, or whether collection was authorized without consent, the purpose for collection must be one that a reasonable person would consider appropriate in the circumstances. Therefore, had the Company obtained consent from all individuals, or the collection was authorized without consent, it would still need to satisfy this second requirement by citing a purpose for collection (or use) that is appropriate in the circumstances.

An appropriate purpose must meet an objective standard considering the context. OIPC orders P12-01[12] and P13-02[13] provide criteria for determining what a reasonable person would consider appropriate. Those criteria include:

[12] 2012 BCIPC No. 25 (CanLII).
[13] 2013 BCIPC No. 24 (CanLII).

1. *Sensitivity of the personal information*

   In some circumstances personal information collected through surveillance may not be particularly sensitive compared to other types of personal information, such as medical or financial information. Nevertheless, when viewed over time surveillance recordings may contain a large amount of personal information.

2. *Amount of personal information collected or used*

   The greater the amount of personal information being collected, the greater the privacy harm associated with its collection. Further, persistent real-time collection of personal information through surveillance has negative psychological and social effects on individuals. Therefore, a purpose for collection is more likely to be appropriate where it requires the collection of the minimal amount of personal information necessary to achieve its objective. In this case, the Company's surveillance operated throughout all employee shifts. The Company did not limit its surveillance in any meaningful manner.

3. *Use of personal information*

   Personal information collected may only be used for purposes for which individuals have been notified and which a reasonable person would consider appropriate. In this case, the Company did not notify individuals of all the potential uses for the personal information it collected via surveillance.

4. *Whether less intrusive alternatives were attempted*

   Surveillance should only be used as an avenue of last resort after other possible solutions have been exhausted. For example, it should not be used to replace adequate training, education and supervision of employees. In this case, the Company acknowledged that no other options were pursued before surveillance was imposed on its employees.

5. *The likelihood of effectiveness in achieving its purpose*

   The collection of personal information will only be authorized where it would be effective for achieving the stated purpose for collection. In order to determine the likelihood that surveillance would achieve this purpose, one must consider the severity of the issue it is intended to prevent, the frequency with which the issue occurs, the sensitivity of the information being collected, and the ability of surveillance to act as a deterrent.

   In this case, the surveillance was not likely to act as a deterrent as the footage was of such a poor quality that, most of the time, it was difficult to determine what particular individuals were doing.

Analysis of the above factors weighs heavily against a reasonable person finding that the surveillance of the Company's employees was appropriate in the circumstances.

As Audit & Compliance Report P16-01 outlines:

> PIPA authorizes the implementation of video surveillance in accordance with the reasonable person test only where there is a real and serious threat to personal safety or security of property, where the organization has tried all reasonable alternatives without success, and where there is a reasonable prospect that the video surveillance will address those threats. As the above examples demonstrate, these conditions must exist prior to the implementation of the video surveillance. Organizations must not collect personal information through video surveillance, proactively, prematurely, out of an abundance of caution or "just in case."[14]

During the investigation, the Company's owner acknowledged there were no prior instances of employee violence, workplace injuries, thefts or other safety concerns that justified the installation of the surveillance system. As well, there was no contractual obligation for the Company to implement a surveillance system of its employees. The Company's owner stated that he implemented surveillance solely based on the recommendation of a crisis management consulting firm.

The Company did not submit that there were any real or serious threats to personal safety or security of property to argue the surveillance was necessary. The Company also did not try any reasonable alternative methods to manage its employees, such as employee training or spot checking the chicken catching operations.

In addition, the surveillance collected by the Company would not be sufficient to defend its reputation. The policy provides that the supervisor determines when the cameras are turned on or off. It is alleged that a prior supervisor witnessed abuse of some chickens and failed to act to prevent it. There is nothing preventing a similarly inclined supervisor from turning off the camera. This, as well as the overall challenges in identifying clearly what people are doing in the surveillance recordings makes it unlikely that the video system is capable of providing meaningful assistance to the Company to defend its reputation.

Moreover, before installing a surveillance system, the Company failed to consider whether less privacy invasive methods were available for their purposes. As per *Audit & Compliance Report P16-01*, PIPA authorizes the implementation of video surveillance in accordance with the reasonable person test, only where there is a real and serious threat to personal safety or the security of property, the organization has tried all reasonable alternatives without success, and there is a reasonable prospect that the video surveillance will address those threats. [15] These conditions must exist prior to the implementation of the surveillance and this was not the case with the Company.

Based on the analysis above, the Company is not authorized under ss. 11 and 14 of PIPA to collect or use the surveillance recordings of its employees, customers or contractors because

[14] 2016 BCIPC 32 (CanLII), at 23.
[15] 2016 BCIPC 25 (CanLII) at 10 and 23.

the recordings were collected for purposes beyond what a reasonable person would consider appropriate in the circumstances. Moreover, the surveillance could not fulfil the purpose that the Company had cited to justify its implementation.

RECOMMENDATION 1

The Company should cease collecting personal information via surveillance.

RECOMMENDATION 2

The Company should destroy all existing records containing personal information collected via its surveillance.

Disclosure of Personal Information

PIPA stipulates that consent is generally required for disclosure of personal information. In addition, an organization may only disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances which fulfill the purposes that the organization disclosed prior to its collection.[16]

During his interview, the Company's owner acknowledged that he showed short clips of the recorded footage to some of his customers. The individuals in the footage had not consented to this disclosure of their personal information, so it was not authorized under PIPA; there was no authority to disclose this information without their consent under s. 18 of PIPA; and disclosing video footage of an employee to a customer in order to improve a Company's reputation is not an appropriate purpose as contemplated by s. 17 of PIPA.

RECOMMENDATION 3

The Company should not disclose any further surveillance to any other organization or individual, unless authorized by PIPA.

[16] Section 17 of PIPA.

Issue 4 – Has the Company complied with its PIPA obligations regarding policies and practices?

Privacy management program

The best way for an organization to demonstrate compliance with PIPA is to implement a privacy management program. Since the Company does not have a privacy management program in place, it should create one tailored to the structure, scale, volume, and sensitivity of the personal information processing activities of the Company.

The principal elements of a privacy management program should include:

- Adequate resources for the development, implementation and monitoring of privacy controls;
- The presence of applicable policies and procedures;
- Up-to-date documentation of risk assessment and mitigation strategies;
- Adequate training delivered regularly;
- Adequate information incident management processes;
- Compliance monitoring; and
- Regular reporting to the executive.

Pursuant to ss. 4 and 5 of PIPA, the Company must develop policies and practices that are necessary to meet its PIPA obligations. To help organizations understand the expectations for PIPA compliance, the OIPC developed a guidance document in collaboration with the Alberta Office of the Information and Privacy Commissioner and the Office of the Privacy Commissioner of Canada.[17]

Accountable privacy management begins with an appropriate framework to ensure adequate protection of personal information in an organization's custody or under their control. The central tenets of a privacy management program include organizational commitment, program controls, ongoing assessment and revision.

Organizations must create and maintain policies and procedures to meet their obligations under PIPA. These policies and procedures should be available to the Company's employees. They should also be tailored to reflect the personal information processing activities of the

[17] The Office of the Privacy Commissioner of Canada (OPC), and the Offices of the Information and Privacy Commissioners (OIPCs) of Alberta and British Columbia, *Getting Accountability Right with a Privacy Management Program*, April 17, 2012, www.oipc.bc.ca.

company. For example, if a new program is introduced that involves collecting personal information in order to deter improper conduct of employees, that new program should be reflected in revised policies and provided to employees. Employees should periodically sign documents acknowledging compliance with those policies.

Getting Accountability Right with a Privacy Management Program states that privacy policies should address the following at a minimum:

- Collection, use and disclosure of personal information, including requirements for consent and notification;
- Access to and correction of personal information;
- Retention and disposal of personal information;
- Responsible use of information and information technology, including administrative, physical and technological controls and appropriate access controls; and
- A process for responding to privacy complaints.

Contrary to the requirements in s. 5 of PIPA, the Company reported that, other than the SOP, it did not have any policies that related to surveillance of people. The SOP only stated that the Company's supervisors would use surveillance and that the Company would retain the surveillance recordings for 30 days. Consequently, the Company's SOP does not constitute an adequate surveillance policy, as the personal information of third parties was also collected through the surveillance, and it is likely the Company processing other personal information such as general employee personal information.

The Company does not have any policies stating the purpose for surveillance nor does it have any notification to its employees that surveillance could be used to manage their employment relationship with the Company. This includes no notice to third parties whose personal information the Company also collected through surveillance.

To achieve compliance with s. 5 of PIPA, the Company must create a privacy policy and provide it to its employees, and policies and practices must be made available to the public, including third parties, on request. As a result of the OIPC's investigation, the Company has already designated its owner as its privacy officer, responsible for ensuring PIPA compliance.

RECOMMENDATION 4

The company should create a privacy policy and procedures that include the following:

a) a statement that personal information is collected in accordance with provisions set out in PIPA;

b) a definition of "personal information" that is consistent with PIPA;

c) an accurate description of:

   i. the personal information that it collects from employees, farmers and contractors;
   ii. the purpose for the collection and use of personal information;
   iii. occasions where the personal information may be disclosed;
   iv. provisions under PIPA for retaining personal information; and
   v. the privacy and security measures used to protect against unauthorized disclosure of personal information (including accurately reflecting access provisions and any physical or technological security controls in place);

d) provisions for obtaining consent for the collection, use or disclosure of personal information that accurately reflect the Company's practices; and

e) additional contact information for the Company's privacy officer, such an email address or telephone number.

RECOMMENDATION 5

The Company should formally review its privacy policy and procedures at least every three years to ensure its policies are relevant and up-to-date.

RECOMMENDATION 6

The Company should create a process for handling privacy complaints, as this is part of the Privacy Officer's responsibilities.

Privacy impact assessment

One of the key components of promoting accountability through a privacy management program is undertaking a privacy impact assessment (PIA) before introducing a new privacy invasive technology into the workplace.

PIAs are internal or external reviews of an organization's compliance with relevant legislation and organizational privacy policies and procedures. They also include verification of the need for collection of each type of personal information and the safeguards employed to ensure that an organization is adequately protecting the personal information it collects. Many of the issues identified would have been evident to the Company had it completed a PIA prior to purchasing a surveillance system.

In this case, the Company assessed the risk of not implementing surveillance. However, it did not assess the privacy risk associated with implementing it.

Similarly, the Company did not consider the privacy impact of the technology on its employees. It is disappointing that the crisis management firm did not suggest that a privacy impact assessment be conducted prior to its recommendation that the Company use surveillance on its employees.

In this case, if the Company had completed a PIA prior to the purchase of a surveillance system, it may have been apparent that this was not a reasonable course of action to take.

RECOMMENDATION 7

The Company should develop formal procedures and conduct privacy impact assessments to ensure that:

a) adequate administrative, physical and technological safeguards are in place to protect the personal information it collects; and

b) collection is limited to only the personal information necessary for the purposes identified.

5.0 SUMMARY OF RECOMMENDATIONS

I have made the following recommendations in this investigation:

RECOMMENDATION 1

The Company should cease collecting personal information via surveillance.

RECOMMENDATION 2

The Company should destroy all existing records containing personal information collected via surveillance.

RECOMMENDATION 3

The Company should not disclose any further surveillance to any other organization or any other individual, unless authorized to do so by PIPA.

RECOMMENDATION 4

The Company should create a privacy policy and procedures that include the following:

a. a statement that personal information is collected in accordance with provisions set out in PIPA;

b. a definition of "personal information" that is consistent with PIPA;

c. an accurate description of:

    i. the personal information that it collects from employees, farmers and contractors;

    ii. the purpose for the collection and use of personal information;

    iii. occasions where the personal information may be disclosed;

    iv. provisions under PIPA for retaining personal information; and

    v. the privacy and security measures used to protect against unauthorized disclosure of personal information (including accurately reflecting access provisions and any physical or technological security controls in place);

d. provisions for obtaining consent for the collection, use or disclosure of personal information that accurately reflect the Company's practices; and

e. additional contact information for the Company's privacy officer, such as an email address or telephone number.

RECOMMENDATION 5

The Company should formally review its privacy policy and procedures at least every three years to ensure its policies are relevant and up-to-date.

RECOMMENDATION 6

The Company should create a process for handling privacy complaints, as this is part of the Privacy Officer's responsibilities.

RECOMMENDATION 7

The Company should develop formal procedures and conduct privacy impact assessments to ensure that:

a. adequate administrative, physical and technological safeguards are in place to protect the personal information it collects; and

b. collection is limited to only the personal information necessary for the purposes identified.

6.0 COMPANY'S RESPONSE

The Company informed the OIPC investigator that the chicken processing and catching industries are moving toward an independent system of audits and third party certifications. Even without the OIPC's investigation, the Company would likely have discontinued surveillance of its employees once the chicken raising and processing industries finalized the accreditation and audit program. To its credit, once the Company was aware of the OIPC's investigation, it stopped video recording its employees.

7.0 CONCLUSION

The key findings detailed in this report included:

1. The Company is collecting personal information when it collects surveillance recordings of individuals as they work on private chicken farms.

2. The information that the Company collected by surveillance in this case does not constitute "employee personal information" under PIPA because the surveillance is not being collected "solely" for that purpose.

3. PIPA does not authorize the Company to collect the personal information of employees, farmers and other contractors via body worn surveillance devices. This is because it did not have consent and it was not authorized under PIPA to collect without consent. Moreover, a reasonable person would not consider the purposes for the collection to be appropriate in the circumstances. For example, there is insufficient evidence of a safety, security or employee management problem, nor evidence of other significant issues that would authorize the Company to monitor and video record employees, farmers and other contractors going about their normal duties. In addition, the Company failed to consider whether less privacy invasive measures were available for their purposes, and the surveillance was unlikely to be effective for the purpose of defending the company's reputation.

4. The company does not have any privacy policies in place that state the purpose for surveillance. It did not notify its employees and non-employees subject to surveillance that it would be collecting their personal information. Finally, it did not conduct a privacy impact assessment.

5. Surveillance equipment has become less expensive and more accessible to broader markets. As a result, many organizations in BC are attracted to using it as a solution to a problem before they have explored all other options, including options that may be more effective and less privacy-invasive.

PIPA authorizes the implementation of video surveillance in accordance with the reasonable person test, only where:

- there is a real and serious threat to personal safety or the security of property,
- the organization has tried all reasonable alternatives without success, and
- there is a reasonable prospect that the video surveillance will address those threats.

Organizations in BC should approach surveillance as a last resort. Too often, organizations, like the one in the case, turn to surveillance thinking it will be a quick and easy solution.

Organizations need to understand the risks that surveillance poses, and take all reasonable efforts to avoid them. This starts with exploring and implementing less privacy invasive alternatives at the outset. Surveillance technologies can be beneficial in the right circumstances, but cause more harm than good when overused.

8.0 ACKNOWLEGEMENTS

The Company cooperated fully with my office's investigation.

I would like to thank Justin Hodkinson, former OIPC Investigator, who conducted this investigation and contributed to this report.