Information and Privacy Commissioner,
Ontario, Canada

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

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT PC11-34

Ministry of Community Safety and Correctional Services

July 3, 2012

Summary: The complainant complained that staff at the Ontario Provincial Police, Lancaster Branch had inappropriately disclosed to her landlord an occurrence report which included her personal information. The ministry responsible for the Ontario Provincial Police admitted that a privacy breach had occurred. The issue here is whether the ministry responded appropriately to this breach, and this Report finds that it did not.

Statutes Considered: *Freedom of Information and Protection of Privacy Act* R.S.O. 1990, c. F.31, as amended, 2(1) definition of personal information, 42(1); R.R.O. 1990, Regulation 460, section 4(1)

Orders and Investigation Reports Considered: HO-010

Cases Considered: *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, [2011] 2 S.C.R. 306

BACKGROUND:

The Office of the Information and Privacy Commissioner/Ontario (IPC) received a privacy complaint under the *Freedom of Information and Protection of Privacy Act* (the *Act*) from an individual (the complainant) concerning the Ministry of Community Safety and Correctional Services (the ministry).

The ministry and the complainant have provided the IPC with following background information concerning this matter.

The complainant was involved in a Landlord and Tenant Board proceeding. In the course of that proceeding, the complainant became aware that staff at her local Ontario Provincial Police (OPP) detachment had provided her landlord with a copy of an occurrence report dated May 4, 2010 which related to an incident involving the complainant. The complainant learned of this when her landlord entered one page of the occurrence report into evidence at the Landlord and Tenant Board hearing on June 3, 2011.

Subsequent to receiving this information, the complainant contacted the ministry to complain about the disclosure and she also filed a complaint with this office.

An internal investigation was conducted by the Professional Standards Bureau (PSB) of the ministry, and the ministry determined that the complainant's landlord had attended the OPP detachment and had a discussion with a clerk about the complainant. The ministry stated that:

> The clerk and the [landlord] knew each other because the clerk works at an OPP detachment, and the individual is a contractor who was formerly contracted by the OPP to clear snow from the OPP premises.

During this discussion about the complainant, the clerk queried the complainant on the OPP Niche Records Management System (Niche RMS), a shared law enforcement database. The clerk retrieved and printed a copy of the occurrence report that contained the complainant's personal information, and showed it to the landlord.

The printing date recorded on the occurrence report is November 5, 2010. However, I note there is a discrepancy regarding the dates because in the letter of apology set out below, the OPP stated that "one of our clerks inappropriately provided a copy of an internal police report" in May, 2010.

Although the clerk was not clear as to what transpired after he showed the occurrence report to the landlord, the ministry informed the IPC that the report was inadvertently mixed in with some other papers of the landlord.

When asked by this office whether the clerk knew that the printed copy of the occurrence report was no longer in his possession, the ministry stated that because the clerk did not recall "disclosing the report" to the landlord, there was no reason for him to know that it was missing.

The ministry also stated that:

> The OPP did not consider any charges against the landlord arising from its investigation because the factual evidence does not suggest that there was intent to commit theft.

During the IPC investigation, the ministry acknowledged that the disclosure of the complainant's personal information was contrary to the *Act*, and at the request of the IPC and the complainant, provided the complainant with a written apology which stated:

> On behalf of the Detachment Commander of the Stormont, Dundas and Glengarry detachment of the Ontario Provincial Police, please accept our sincere apology for the inappropriate release of information relating to your complaint.
>
> In May 2010, one of our clerks inappropriately provided a copy of an internal police report in relation to occurrence # [ ] contrary to the Freedom of Information and Protection of Privacy Act. Subsequently, all the administrative clerical members of the Detachment have been provided with specific guidelines with respect to the release of personal information.
>
> We regret any difficulty that this has created and we believe that our response will see to it that this does not occur again.

Upon receiving the apology letter, the complainant advised this office that she was not satisfied that her complaint had been dealt with appropriately by the ministry. Specifically, the complainant felt that the ministry had not taken the appropriate steps in response to the breach in that it failed to provide her with a detailed explanation about the circumstances surrounding the breach, including the actions taken against the clerk, and it failed to take appropriate steps to ensure a similar incident would not re-occur.

The IPC issued a draft report on May 4, 2012, and the complainant and ministry were each provided an opportunity to comment on the draft. Concurrently, the file was assigned to me as the Investigator. Subsequently, both the complainant and the ministry provided me with their comments in response to the draft report.

I have carefully considered all of the comments received by the parties and the correspondence and other documentation and information provided by the ministry and the complainant both before and after the issuance of the draft report. I have taken all of the information and arguments provided into consideration in preparing this final report.

DISCUSSION:

The following issues were identified as arising from the IPC investigation:

Did the occurrence report contain "personal information" as defined in section 2(1) of the *Act*?

"Personal information" is defined in section 2(1) which states, in part:

> "personal information" means recorded information about an identifiable individual, including,
>
> ...

> (h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual…

It is important to note that occurrence reports such as the one at issue here include highly sensitive and often detailed information about police incidents, as well as information about individuals such as the names of complainants, witnesses and victims, and other highly sensitive information about people, who may or may not have been charged with a crime.

I have reviewed the occurrence report and I find that it identifies the complainant by name and contains details of an OPP officer's interview with the complainant. In these circumstances, I am satisfied that the occurrence report contains personal information as defined in section 2(1) of the *Act*. The ministry does not dispute this finding.

As an aside, because there was some discrepancy in the information provided to this office, the ministry was asked to clarify the number of pages in the occurrence report at issue. Since the issuance of the draft report, the ministry has confirmed that the occurrence report is two pages in length but that the second page of the report is blank.

Was the disclosure of the "personal information" in accordance with section 42(1) of the *Act*?

Section 42(1) of the *Act* provides a general prohibition against disclosure of personal information in the custody of an institution unless the circumstances fall within one of the exceptions in the *Act*.

While the ministry has not denied that an inappropriate disclosure took place in this investigation, in my view, the following information which was provided to this office about the circumstances of the disclosure is relevant.

Following the issuance of the letter of apology in which the ministry admitted to the inappropriate disclosure, ministry counsel advised the IPC of the following:

> [A]ll the evidence that we have points to a lone clerk in one OPP detachment inappropriately disclosing personal information contained in a two page general occurrence report about a landlord and tenant dispute on the mistaken belief that such disclosure was permissible. This mistaken belief was based on the clerk not receiving adequate training, which we have since addressed. While we realize that this is a serious incident, which necessitated decisive action on our part, we do not believe that it comes close to being wilful or intentional.

Subsequently, in response to a formal request for information, the ministry stated:

> An individual attended at the Lancaster satellite office of the OPP, which is part of the Stormont, Dundas and Glengary detachment. The individual had a discussion with the clerk about the complainant, which led to the clerk querying

> the complainant on the OPP Niche Records Management system (NICHE RMS), a shared law enforcement data base.
>
> The clerk retrieved and printed off a copy of an occurrence report that contained the complainant's personal information, and showed it to the individual. The individual somehow left the detachment with a printed copy of the report. The clerk told the OPP investigator that he does not recall disclosing the report to the individual and claims that it was inadvertently mixed in with some other papers that the individual had in his possession at the time. The individual subsequently used the occurrence report at a tribunal hearing.

I note that while the clerk indicated that he could not recall "disclosing" the report to the landlord, he does admit that he "showed" it to the landlord.

Regardless of the circumstances that led to the clerk providing or "showing" the complainant's landlord a copy of the report, I find that the clerk disclosed the report which included the complainant's personal information and, in light of the ministry's acknowledgement of the privacy breach, I find that the disclosure was not in accordance with section 42(1) of the *Act*.

Did the ministry comply with section 4(1) of Ontario Regulation 460, made pursuant to the *Act*, by ensuring that "reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected"?

Section 4(1) of Ontario Regulation 460, made pursuant to the *Act*, outlines the obligation of the heads of institutions to ensure they have reasonable measures in place to prevent unauthorized access to the records in his or her institution. Section 4(1) states:

> **4.** (1) Every head shall ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected.

In the discussion that follows, I will consider whether the ministry has complied with the *Act* by having reasonable measures in place to prevent unauthorized access to records of personal information, taking into account the nature of the records to be protected.

Disclosure of information surrounding the breach and discipline

As noted above, the circumstances of this breach involve a clerk accessing an occurrence report about the complainant, printing it and showing it to the complainant's landlord. It is alleged by the ministry that subsequent to this unauthorized disclosure, the report disappeared and the clerk does not know how that happened.

I have already found that the record disclosed contained the personal information of the complainant, and that this disclosure was contrary to the *Act*.

As mentioned previously, after receiving a written apology for the disclosure from the ministry, the complainant advised this office that she was not satisfied that her complaint had been dealt with appropriately by the ministry. Specifically, the complainant felt that the ministry had not taken the appropriate steps in response to the breach in that it failed to provide her with an explanation about the circumstances surrounding the breach, including the actions taken against the clerk, and it failed to take appropriate steps to ensure a similar incident would not re-occur.

Consequently, the IPC contacted the ministry and requested that it provide to the complainant further details regarding the steps the ministry had taken as a result of the disclosure of this occurrence report, including the remedial steps taken with respect to the clerk involved. The ministry however declined.

Subsequent to the ministry's refusal to do so, the IPC wrote to the ministry with a formal request for information. In the request for information, the IPC asked several questions including the following:

> Please advise what steps the ministry took, or is taking, in response to the disclosure of the complainant's personal information. In particular, please comment in detail on the complainant's request for:
>
> …
>
> b. confirmation that appropriate actions were taken by the ministry vis-à-vis the clerk as a consequence of the breach; and,
> c. an explanation and apology as to the length of time taken by the Ministry to issue an apology to the complainant.

The ministry responded as follows:

> (b) *Confirmation that appropriate actions were taken* – We confirm that the Ministry has taken appropriate actions vis-à-vis the clerk as a consequence of the breach.
>
> (c) *Explanation and Apology* – The OPP has acted appropriately in investigating this breach, and in taking remedial steps.

This office was not satisfied with the response, and the previously assigned investigator wrote back to the ministry and asked, what steps the ministry took or is taking in relation to the clerk's inappropriate disclosure and/or showing of the occurrence report to the individual. In addition, the investigator advised the ministry that this question related specifically to the clerk involved, and that the response should include information about disciplinary or remedial steps taken or that will be taken against the clerk, if any. In responding to this question, the ministry stated:

> …clerks at the detachment received a power point presentation, and a Privacy Basics e-course. In addition, the clerks were reminded of their confidentiality obligations under the OPP Police Orders.

> With respect to the clerk who retrieved the occurrence report, he was counselled at length by his manager, and a human resources advisor about his obligation to protect privacy.

Despite the information provided to the IPC in response to this investigation, in my view, the ministry's initial response to the circumstances of this privacy breach was not adequate. In my opinion, the ministry's failure to disclose the details of the breach and the disciplinary action, if any, following discovery of the breach, to the complainant amounts to a failure to implement reasonable measures to prevent unauthorized access. I also note that this information was not provided to this office without some prodding.

Giving employees wide and rapid access to computer databases containing sensitive personal information may be necessary and essential; this is particularly so in a law enforcement context where incidents that impact the health and safety of individuals need immediate attention, and where the health and safety of responding officers may also be at risk. However, knowing that wide and rapid access to these databases is essential, the ministry is required to take reasonable measures to ensure that its employees do not abuse their access rights and privileges, and to ensure that employees understand their obligations to protect the privacy and security of personal information and understand the consequences of their failure to do so.

In my opinion, in circumstances such as these, institutions should disclose detailed information about the privacy breach and the disciplinary action taken to the victim of the breach. While this office will not comment on the adequacy of the disciplinary action, if any, the disclosure of this information to an affected individual may serve two purposes. First, it may act as a deterrent to other staff who are entrusted with the privacy of the personal information of members of the public.

In addition, it may reassure the affected individual(s), and other members of the public who have entrusted their personal information with that institution, that the institution will take the necessary steps to ensure that this type of conduct is not repeated. This is particularly important in the context of a privacy breach such as this one which involves highly sensitive personal information. Moreover, this approach accounts for the fact that the citizens of Ontario do not have the option of dealing with another police force, if they find that their personal information has not been appropriately protected.

The circumstances of this complaint are analogous to those at issue in Order HO-010, issued under the *Personal Health Information Protection Act (PHIPA).* Order HO-010 dealt with a claim that a staff member of a health information custodian had inappropriately accessed a patient's personal health information. Consequently, one of the issues under investigation in Order HO-010 was whether the health information custodian had complied with section 12(1) of the *PHIPA* which outlines the obligation of health information custodians to protect personal health information. It states:

> A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal.

Like the circumstances here, Order HO-010 dealt with an inappropriate disclosure by a staff member. In my view, the findings made in Order HO-010 offer some guidance regarding the approach to be taken to determine the ministry's obligations under section 4(1) of Regulation 460.

The circumstances in Order HO-010 were that, on being notified of the breach, the hospital conducted an investigation which culminated with the issuance of a letter to the complainant apologizing for the breach. However, the complainant was not given any information as to whether or not the staff person involved was disciplined. The complainant was not satisfied with the response she received and filed a complaint with this office.

The IPC conducted an investigation under *PHIPA,* and at the conclusion of that investigation Order HO-010 was issued. In that Order, Commissioner Cavoukian stated*:*

> Other than reporting to the complainant regarding the results of the audits conducted, the complainant was provided with limited information regarding the actions taken to address this incident. In my view, the complainant has a right to this information – she was the victim of a breach of the *Act* that was confirmed and acknowledged by the hospital. The complainant has a right to receive assurances that the incident has been appropriately addressed and that steps have been taken to prevent its re-occurrence. Critical to this assurance are details of the steps taken by the hospital, including the results of its investigation and the fact that disciplinary action was taken against the employee in question.

In a postscript to Order HO-010, Commissioner Cavoukian added:

> This level of transparency is important for several reasons. Accessing a patient's personal health information in an unauthorized manner is a serious violation of an individual's privacy and security of the person. In such a situation, the aggrieved individual has a right to a complete accounting of what has occurred. In many cases, the aggrieved parties will not find closure regarding the incident unless all the details of the investigation have been disclosed. Receiving general assurances that "the incident has been dealt with appropriately" falls far short of the level of disclosure that is required.
>
> For other staff members of the hospital involved, knowing that all of the details of the disciplinary action imposed will be publicly disclosed, should serve as a strong deterrent. This is especially true if those details also become known to other employees, either through the actions of the aggrieved individual, the custodian, or both. Employees must understand that, given the seriousness of these types of breaches, their own privacy concerns will take a back seat to the legitimate needs of the victims involved to have a full accounting of the actions taken by the health information custodian. Our primary concern must lie with the aggrieved party, whose privacy was completely disregarded.

Turning to this complaint, in its response to the draft report, the ministry expressed that the IPC appeared not to have considered the ministry's submissions "as to why the factual circumstances in Order HO-010 are different than those at issue in this privacy complaint."

While all of the ministry's comments provided in this investigation were considered in the preparation of the draft report and have been considered by me in this report, I will set out the specific arguments raised about the import of Order HO-010 here.

By letter dated January 25, 2011, the ministry stated that there is a distinction between the circumstances in this complaint and those in Order HO-010. Specifically, counsel for the ministry stated:

> You have cited Order HO-010 in support of your position. However, the facts giving rise to that Order are completely different and distinguishable from this complaint. In Order HO-010, the Information and Privacy Commissioner found that a hospital technologist intentionally chose to access a record containing personal health information marked with a "sensitive flag warning" in "blatant disregard" of hospital policy. This unauthorized access occurred on six separate occasions over a nine month period, and on three of those occasions, the technologist viewed over twenty screens of data at each access point. Moreover, the technologist was the former spouse of the complainant's current spouse, pointing to a serious conflict between the technologist's occupational duties and her desire to find out personal information about her spouse's former partner.
>
> …
>
> …we do not quarrel with the conclusions reached in Order HO-10 … where reference to disciplinary action was based on the particular factual circumstances … However, we do not believe that the facts of this complaint are at all analogous. We do not believe in particular that you have fully considered the following:
>
> - The clerk appeared to have acted alone, and made a single error on one occasion resulting in the disclosure of a single record. We believe that this mistake was due to a lack of training, rather than as a result of malice or intent. We do not believe that this disclosure represents a systemic failure on the part of the OPP to protect personal information.
>
> - The clerk works in a small OPP detachment in rural Ontario. Any disclosure of personal information even where it does not identify the clerk by name must nevertheless be considered in terms of the harm it could cause, given the size of the detachment and the community it serves. The clerk also has privacy rights, and these need to be taken into account based on the specific facts of the complaint.

While I acknowledge that there are differences in the circumstances surrounding the breach of privacy that occurred in Order HO-010 and the circumstances that are before me in this complaint, I remain of the view that the findings made in that Order offer some guidance here. In my view the Commissioner's findings and comments regarding the right of a victim of a privacy breach to full disclosure of the institution's response to the privacy breach, and the Commissioner's comments regarding the impact that a practice of full disclosure of the response may have on other staff, apply equally here for the following reasons.

This complainant is a resident of the community served by the OPP detachment where the privacy breach occurred. She is entitled to assurances that her personal information will not be the subject of any further inappropriate disclosures by staff at this detachment. She should also be entitled to assurances that if she requires the assistance of staff in this detachment at any time, including in relation to matters that may affect her own personal health and safety, she can provide her personal information to OPP staff knowing that it will be secure from inappropriate disclosures by clerical staff or members of the police force.

If an institution has a policy or practice of disclosing, barring exceptional circumstances, the details of its response to a privacy breach this may deter staff from disclosing information without the appropriate authority to do so. In my view, the implementation of such a policy or practice is a reasonable measure.

Accordingly, I find that the obligation set out in section 4(1) of Regulation 460 to put in place reasonable measures to protect personal information from unauthorized disclosure, includes an obligation, barring exceptional circumstances, which are not apparent here, to provide the affected individual with the details of the steps taken in response to the breach, including the results of the internal investigation and any disciplinary action taken against the employee in question.

In his response to the draft report, ministry counsel stated that this interpretation of section 4(1) was not consistent with the approach taken to statutory interpretation adopted by the Supreme Court of Canada, and he cited the case of *Canada (Information Commissioner) v. Canada (Minister of National Defence)*, 2011 SCC 25 in support of his position. Ministry Counsel also made the following comments regarding section 4(1) of Regulation 460:

> The report fails to consider the fact that section 4(1) is part of a regulation, and a regulation is subordinate form of legislation, meaning that it must be read in 'in context' as being subordinate to the statue. The [*Act*] explicitly excludes most labour and employment related records in which the Ministry "*has an interest*". In other words, section 4 must be read as part of the legislative scheme in [the *Act*], and that scheme does not apply to records such as those that give rise to this complaint.

Ministry counsel went on to state the following:

> Similarly, the report fails to address the profound inconsistency between the recommendations in the report to disclose a disciplinary record, and the fact that this same record is not subject to the jurisdiction of [the *Act*]. It does not make sense in our view for a record to be recommended for disclosure pursuant to a privacy complaint report that is otherwise inaccessible under the same statute.
>
> The Ministry is not aware of section 4(1) ever being interpreted so as to recommend the disclosure of disciplinary action taken against an employee. An ordinary reading of section 4(1) does not support this interpretation.

I disagree with the ministry's view that there is any inconsistency in the recommendation to disclose the disciplinary action. I recognize that as a general rule, the *Act* does not apply to

labour or employment related records and therefore, the access and privacy provisions of the *Act* do not apply to records of this nature. The exclusion in the *Act* for records of this nature does not however, limit the ministry's ability to provide victims of a privacy breach with information about the actions taken to respond to the breach, including the nature of the disciplinary action taken. Section 65(1)(a) does not prevent or prohibit an institution from disclosing this information, pursuant to a policy or practice. Therefore, there is no inconsistency as the ministry suggests.

Furthermore, while the obligation to make a full disclosure to a victim of a privacy breach stems from the ministry's obligations to ensure that it has reasonable measures in place to prevent unauthorized access to records in its custody pursuant to section 4(1), in my view, the obligation to disclose these details is also a privacy best practices.

This approach is analogous to the approach taken by this office to the issue of notification. For example, despite the fact that the *Act* does not include a mandatory breach notification provision, this office has advised institutions in Ontario, that barring exceptional circumstances, an institution should notify affected individuals in the event of a privacy breach as a privacy best practice. For example, this office's "Privacy Breach Protocols: Guidelines for Government Organizations" recommends that, in the event of a privacy breach, institutions should:

> Identify those individuals whose privacy was breached and, barring exceptional circumstances, notify those individuals accordingly.[1]

This is a recommendation that has been widely accepted by institutions in Ontario.

In the same publication, this office advises that an institution should tell the victim of the privacy breach what steps have been taken to address the breach, both immediate and long term. In circumstances such as those before me here, in setting out the steps taken to address the breach, the victim should also be told, barring exceptional circumstances, what steps have been taken to discipline the employee involved as this is a privacy best practice and may be a critical component to an organization's response to the breach.

For all of these reasons, I find that in the circumstances of this complaint, the ministry should have disclosed the full details of its response to the privacy breach, including the details of any disciplinary action taken against the employee involved.

Policies and Procedures

As section 4(1) requires the head of the ministry to ensure that reasonable measures to prevent unauthorized access to the records in his or her institution are defined, documented and put in place, taking into account the nature of the records to be protected, I now turn to review the relevant policies and procedures of the ministry.

In the request for information, the IPC asked the ministry whether it has adopted measures to protect its records of personal information, and what those measures are. The IPC also asked for copies of all policies, procedures and practices to support the ministry's position. In

[1] http://www.ipc.on.ca/images/Resources/Privacy-Breach-e.pdf

response to the request, the ministry provided a number of documents. Of these documents, I find that the following policies and procedures are relevant to this matter:

- "Corporate Policy on Protection of Personal Information"
- "Best Practices for Responding to a Privacy Breach"
- "Taking the Right Steps – A Guide to Managing Privacy and Privacy Breaches"
- Relevant portions of "Niche Records Management System Standard Operating Procedures Manual" – pages 1-8 and 40-41
- Relevant Ontario Provincial Police Orders.

The "Corporate Policy on Protection of Personal Information", "Best Practices for Responding to a Privacy Breach" and "Taking the Right Steps - A Guide to Managing Privacy and Privacy Breaches" were developed by the Ministry of Government Services (MGS). The ministry advised that it has not developed its own privacy breach protocols and that it follows these policies which were issued by the Office of the Chief Information and Privacy Officer of MGS.

On their face, these policies appear to be sufficient as a guide to privacy and privacy breaches and privacy breach management for senior staff and FOI coordinators. From the information provided by the ministry in response to the draft report, I note that these policies are accessible to front line staff such as the clerk "via computer access".

With regards to the policies listed above, the Niche RMS manual, the police orders and the "Best Practices for Responding to Privacy Breaches" are the only policies that inform staff such as the clerk. While the remainder of the policies listed may be accessible to staff "via computer access" and may be adequate for the purposes for which senior staff and freedom of information coordinators require, it is not clear how these policies inform frontline staff such as the clerk.

For example, the document "Taking the Right Steps - A Guide to Managing Privacy and Privacy Breaches" is addressed to institutions. Its stated purpose is to help institutions:

> Prevent, prepare for and respond to any incident involving unauthorized disclosure of personal information (i.e., a privacy breach).

The guide has two parts. Regarding part 1, the guide states:

> This Part will be of particular interest to Chief Administrative Officers and Delegated Decision-Makers responsible for the protection of privacy within institutions.

Regarding part 2, the guide states:

> This part will be of particular interest and use to institutions' Freedom of Information and Privacy Coordinators (Coordinators) and Program Managers responsible for responding to privacy breaches.

In my view, this guide does not sufficiently speak to the work and needs of front line staff like the clerk and their obligations under the *Act* to protect privacy.

The stated goal of the "Corporate Policy on Protection of Personal Information" is to "define and establish requirements consistent with the [*Act*], for the protection of personal information in the custody or under the control of government." Again, a review of this document indicates that it is primarily addressed to senior staff and not frontline employees such as the clerk and therefore it is not sufficient for the purposes of front line staff who have day to day access to highly sensitive personal information.

Having reviewed the two policies and for the reasons set out above, I find that they do not offer sufficient guidance or other information necessary for clerical and detachment staff to understand their obligations to protect the privacy rights of the individuals whose information is contained in the records that they have access to on a daily basis.

Best Practices for Responding to Privacy Breaches

The "Best Practices for Responding to Privacy Breaches" is a one page document addressed to staff at several levels, including clerical and detachment staff. The document describes a privacy breach as "an incident involving unauthorized disclosure of personal information in the custody or control of a ministry (e.g., mailing a letter to the wrong person)." It addresses ministry staff such as the clerk in this instance when it requires the reporting of "all privacy breaches or suspected breaches to your manager. Managers will report breaches to the FIPPA Coordinator who, in turn will report them to appropriate parties." In my view the remainder of the document is addressed to more senior staff who are to coordinate a response to a privacy breach including notifying affected individuals, investigating the circumstances surrounding a breach and implementing changes.

I find that the amount of information in this document provides minimal guidance to clerical and detachment staff. While the description of a privacy breach and the accompanying example are helpful, much more information is needed to instruct staff regarding what constitutes personal information and inappropriate disclosure and emphasizing the highly sensitive nature of the personal information in the custody of the ministry. The circumstances of this complaint illustrate the point perfectly. The ministry explained that the clerk permitted the landlord to look at the occurrence report, yet apparently did not believe this was a disclosure.

Niche Records Management System Operating Manual

The Niche RMS is the database that was accessed by the clerk and was the subject of the breach. This database is an information management system which contains detailed and sensitive information such as the occurrence report at issue here. It is a shared system in that other police forces have access to it.

The ministry stated that OPP clerks require access to Niche RMS to "maintain an organized, up-to-date records system and to locate and correctly file documents." The ministry explained that a clerk will often access Niche RMS as a result of an inquiry from a member of the public to determine, for example, who in the OPP should receive, and respond to an inquiry.

From my review of the portions of the manual that were provided to me, I note that it is an operating procedures manual that sets out the operational rules for the use and access to the

database. The manual includes some general information about access rights under the *Act* and some general information identifying staff responsible for processing access requests.

Elsewhere, in the portions of the manual that were provided to me, there is reference to security of the information contained in the system and a passing reference to confidentiality. For example, there is a reference to the fact that information contained in Niche RMS should not be released to any "unauthorized person."

It is apparent that although this manual makes reference to the *Act,* it focuses on access and neglects to mention that individuals whose information it contains have a right to privacy with respect to the highly sensitive information stored on this system.

If clerical staff in OPP detachments are trained using this manual, then the manual or an addendum to the manual needs to speak directly to the privacy and confidentiality rights of the individuals whose sensitive information is contained in the database. The failure of the ministry to specifically address this in the Niche RMS manual is not consistent with its obligations under section 4(1) of Regulation 460 and I will recommend that the ministry revise the manual or develop an addendum that addresses the issues of privacy and confidentiality.

Police Orders

As noted above, the ministry provided the IPC with a number of police orders which it stated include its policies on privacy. The ministry takes the position that these police orders are confidential and should not be shared, and therefore I am unable to describe the information that they contain in any detail.

However, it is fair to state that while these orders refer to an individual's right of access under the *Act,* and they advise staff as to where to direct individuals who seek access to records under the *Act*, these orders only make general references to obligations to maintain the confidentiality of records in the Niche RMS, and the obligation to protect individual privacy.

The orders do not include a definition of personal information, an explanation of the right of privacy and they do not define a privacy breach. Consequently, staff referring to these police orders would have no information to assist them in understanding the obligation to protect the privacy of personal information, and in identifying a privacy breach and understanding how to respond to it at a staff level.

The management of privacy needs to be an institution-wide initiative, and needs to involve all staff who use and have access to the sensitive personal information entrusted to them.

In my view, and for the reasons set out above, neither the Niche RMS manual, nor the police orders, nor the "Best Practices for Responding to Privacy Breaches" which are the only policies that appear to apply to staff such as the clerk, are sufficient to prevent unauthorized access as required by section 4(1) of Regulation 460. Consequently, I will recommend that the ministry conduct a review of its policies to address the issues raised in this report.

Training

The requirement to put in place reasonable measures to protect information from unauthorized access pursuant to section 4(1) includes a requirement to ensure that staff are appropriately trained in the management of personal information. This means that staff and management who require access to personal information in order to perform their duties shall receive training to a level commensurate with the sensitivity of the information to which they have access.

In response to my request for copies of any relevant training materials, and details as to how the training is conducted, when the last training was conducted and how often the training is repeated for the clerk and other staff in that office, the ministry provided the following information:

> The Government of Ontario has developed an on-line e-course titled 'Privacy Basics'. The FOI office has previously provided you with a copy of the outline of it, but we are attaching it for your reference. All clerical members of the Stormont, Dundas and Glengary OPP detachment (which includes the Lancaster satellite office) *took this course following the inappropriate disclosure that is the subject of this complaint.* The course takes approximately 2 hours to complete.
>
> Further to the above noted e-training, the East Region of the OPP has undertaken classroom training sessions aimed at educating clerical staff across the region with respect to their responsibilities under the *Freedom of Information and Protection of Privacy Act.* The first of two classroom session occurred on February 1, 2012, and a second classroom session is planned for April 2012. I am providing you with a copy of training materials provided by OPP Risk Management for the first session. [Emphasis added.]

In addition, copies of the following training materials were provided to me:

- "Freedom of Information…and other requests" – a powerpoint presentation
- "Privacy Basics e-course."

This office was not provided with any further information about the ministry training program other than what is set out above.

At the outset, I note that the Freedom of Information powerpoint presentation focuses on access rights and therefore, in my view, does not qualify as appropriate privacy training.

In response to the draft report, the ministry made the following comments about the e-course:

> The report states that the Privacy Basics e-course was "only offered to the clerk and other staff in the detachment following the discovery of this privacy breach." This is incorrect. The e-course was available beforehand, but it was only mandated after the breach.

I have reviewed the Privacy Basics e-course and, in my view, it is a reasonably good training tool. While the course may have been available before the breach, I note that since this

complaint was filed, the ministry has changed its practices and the course is now "mandated." I commend the ministry for taking this initiative. I also commend the ministry for offering the course to all clerical staff in the detachment as part of its response to this privacy breach.

However, the ministry does not indicate whether or not this course will form part of the ministry's orientation of new clerical staff, or whether it has plans to require that the training be repeated at any time during the course of the employment.

In my view, the ministry training practices and materials should be reviewed to ensure compliance with ministry obligations under the *Act*. While an institution may have strong privacy policies, if staff have not been adequately trained, those protocols are of little assistance in ensuring the confidentiality and security of personal information.

It is significant that the ministry has on its own initiative identified the lack of training as an issue. In its response to requests for information in this complaint, ministry counsel stated:

> [A]ll the evidence that we have points to a lone clerk in one OPP detachment inappropriately disclosing personal information contained in a two page general occurrence report about a landlord and tenant dispute on the mistaken belief that such disclosure was permissible. This mistaken belief was based on the clerk not receiving adequate training, which we have since addressed.

Subsequently, in response to the draft report, ministry counsel stated:

> The clerk appeared to have acted alone, and made a single error on one occasion resulting in the disclosure of a single record. We believe that this mistake was due to a lack of training, rather than as a result of malice or intent.

For these reasons, I find that the ministry should strengthen its personal information and privacy training program to comply with its obligations under section 4(1) of Regulation 460.

CONCLUSIONS:

1. The occurrence report in question qualifies as personal information as defined in section 2(1) of the *Act*.

2. The disclosure of the personal information was not in accordance with section 42(1).

3. The ministry should have exercised its discretion to provide the complainant with information regarding any disciplinary action taken as a result of the privacy breach.

4. The ministry should review and revise its privacy policies, procedures and practices.

5. The ministry should establish a training program in accordance with the recommendations set out below.

RECOMMENDATIONS:

I recommend that the ministry:

1. Advise the complainant what, if any, disciplinary actions were taken against the clerk who was responsible for the breach of the complainant's privacy.

2. Review and revise its policies and procedures relating to the privacy of personal information to ensure that they comply with the requirements of the *Act* and its regulations, taking into account the concerns expressed in this report.

3. Establish a training program which will require all clerical staff handling sensitive personal information to undergo privacy training at hiring, and will require that the training be repeated at regular intervals. This training program must include general privacy and security awareness, and specific training related to information systems, including the Niche RMS, used by the ministry.

4. Within 90 days of publication of this report, give the Information and Privacy Commissioner a written plan setting out the ministry's commitment and plan to comply with recommendations 1, 2 and 3 as outlined above.

July 3, 2012

Jeffrey Cutler
Investigator