



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

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NO. PC07-41, PC07-45,
MC07-29 and MC07-33

Ministry of the Attorney General
Ministry of Community Safety and Correctional Services
City of Toronto
Toronto Police Services Board



Tribunal Services Department
2 Bloor Street East
Suite 1400
Toronto, Ontario
Canada M4W 1A8

Services de tribunal administratif
2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
Canada M4W 1A8

Tel: 416-326-3333
1-800-387-0073
Fax/Télééc: 416-325-9188
TTY: 416-325-7539
<http://www.ipc.on.ca>

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NO. **PC07-41, PC07-45, MC07-29
and MC07-33**

INVESTIGATOR: **Mark Ratner**

INSTITUTION: **Ministry of the Attorney General**

SUMMARY OF COMMISSIONER INITIATED COMPLAINT:

Nature of the Incident

On May 4, 2007, the Office of the Information and Privacy Commissioner/Ontario (IPC) was contacted by a Global TV news reporter regarding a potential privacy breach (the incident) at the Old City Hall (OCH) Courthouse in Toronto. The reporter informed the IPC that un-shredded court documents containing identifiable information were found on the curb outside of OCH in clear plastic bags, and that Global TV would be broadcasting a story about the incident on its evening newscast. That evening, a story was broadcast providing details regarding the incident.

Based on this information provided to the IPC and the subsequent news report, the IPC immediately initiated an investigation into the matter under the *Freedom of Information and Protection of Privacy Act* (the provincial *Act*) and the *Municipal Freedom of Information and Protection of Privacy Act* (the municipal *Act*).

The IPC immediately contacted the Ministry of the Attorney General (MAG) as the provincial ministry responsible for court operations in the province to request that the bags be removed from the curb and be taken to a secure location. In addition, an investigator from the IPC attended at OCH to assess the scope of the breach. Upon arrival, the investigator was informed that the bags in question had already been picked up in accordance with the regular garbage and recycling pickup schedules, and had been taken to a city transfer station. Because the garbage and recycling had already been picked up, it was no longer possible to secure the records in question, or determine whether they contained personal information. In addition, because the records had already been removed, it was not possible to identify the affected individuals, if any, and notify these individuals that their personal information may have been compromised.

During the May 4, 2007 site visit, the IPC met with representatives from MAG's Court Services Division as well as MAG's Freedom of Information department. Staff from the City of Toronto (the City's) Facilities Services department were also present at the meeting.

During this meeting, MAG staff explained that garbage and recycling pickup within OCH is handled by the City's Facilities Services staff, who are responsible for collecting the garbage and recycling from all offices within OCH and for holding these materials in the OCH courtyard to await the scheduled pickup dates. On the evening before pickup, the garbage and recycling is moved to the Albert Street curb on the north side of the building to await pickup. Staff stated that the records in question were likely viewed by the television reporter at this curb location prior to pickup.

With respect to the source of the potential breach within OCH, MAG staff indicated that garbage and recycling within OCH is generated by a variety of stakeholders including government offices within the building, private agencies, Judges and Justices of the Peace, as well as the general public. Consequently, MAG staff indicated that it would be difficult to identify the specific source(s) within OCH of the breach. MAG provided the IPC with a list of stakeholders who occupied space in OCH.

Records found on site

Although the records that had been left on the Albert Street curb had been picked up by the time the IPC investigator arrived at the OCH site on May 4, 2007, a small amount of recycling and garbage had accumulated in the OCH courtyard by the time the visit took place. Samples of these records containing personal information were collected from the site.

During a subsequent site visit, additional samples of records that had been set aside for garbage or recycling pickup were taken from the courtyard. Included among the records were the following records containing names of individuals:

- Notice of Assignment Court
- Notice of Intention
- Drug History Card
- Pre-hearing Conference Report Form
- Bench Warrant Certificate Form
- Warrant for Arrest

In response to this complaint, MAG provided the IPC with a copy of its own internal investigation report into the incident. In this report, MAG provided an explanation of the potential uses of the records that were located on site. The report noted that some of the records, such as the "Notice of Assignment Court" or the "Pre-hearing Conference Report Form" are records that are normally provided to accused persons. The report further noted that other records, such as the "Drug History Card" and "Notice of Intention" appeared to relate to Federal Crown matters. The report further stated:

Although some of the documents appear to be court documents or Ministry type documents, some of these types of documents originate from different organizations and are given to numerous organizations and individuals in OCH ... Therefore, it is impossible to control its eventual disposal by individuals or organizations outside the Ministry or to ascertain who has placed them in the recycling dumpsters.

Conduct of the investigation

In conducting this investigation, I am mindful of the uncertainty regarding the source of the breach. With respect to the clear plastic bags, I note that these bags were taken away prior to the start of the investigation and could not be examined. With respect to the records collected at the site, I am in agreement with the conclusions outlined in MAG's internal investigation that it is not possible to ascertain **who**, or **which department** had placed these records into the disposal system.

Due to the uncertainty with respect to the source of the breach, the IPC proceeded to investigate the information security and destruction practices at each of the offices, in operation at OCH, that qualify as an "institution" under either section 2(1) of the provincial *Act* or section 2(1) of the municipal *Act*.

The purpose of this investigation is to assess the information destruction practices currently in place at OCH with a view to determining whether these practices can be improved upon so as to reduce the risk of similar incidents occurring in the future.

The IPC's position on information destruction has been expressed in the Fact Sheet titled *Secure Destruction of Personal Information*¹ (the Fact Sheet) which states that all records containing personal information must be destroyed in a secure manner. With respect to paper records, the Fact Sheet recommends that all records containing personal information be destroyed through shredding.

The following offices that operate at OCH fall under the definition of "institution" under section 2(1) of either the provincial *Act* or the municipal *Act*:

The Ministry of the Attorney General

- Court Services Division offices
- Crown Attorney's offices
- Victim Witness Assistance Program

The City of Toronto

- Legal (Prosecutions Unit)
- City of Toronto Court Services
- Facilities Services/Custodial

¹ http://www.ipc.on.ca/images/Resources/up-fact_10_e.pdf .

The Ministry of Community Safety and Correctional Services

- Probation and Parole office

The Toronto Police Service

- OCH Unit

Accordingly, Commissioner-initiated privacy complaint files were opened with the Toronto Police Service (TPS), the Ministry of Community Safety and Correctional Services (MCSCS), the City, and MAG.

During this investigation, each of the four institutions was asked to provide its respective position on the complaint and to specifically address the following:

1. Whether the institution's offices at OCH had a written policy in place setting out appropriate records destruction practices;
2. The manner in which any policies are disseminated to staff;
3. Whether the institution's offices at OCH are laid out in a manner that facilitates the secure destruction of personal information; and
4. Where service providers had been retained to provide information destruction services, whether contracts were in place containing appropriate clauses to provide for secure destruction.

In addition, the IPC had further meetings with the City (as the owner of OCH) and MAG (as its primary tenant) to discuss their respective positions on the complaint.

DISCUSSION:

The following issues were identified as arising from the investigation:

Are the records in question subject to the provincial *Act* and the municipal *Act*?

The first step in the analysis is to determine whether the records in question are subject to the provincial *Act* and the municipal *Act*, respectively.

Because the primary function of OCH is as a court house, some of the records that are processed therein can properly be considered to be "court records". In Order P-994, the IPC considered whether court records that are processed by MAG are properly considered to be under the custody or control of that institution, and therefore subject to the provincial *Act*.

In addressing this question, Inquiry Officer Laurel Cropley stated:

I have carefully considered the Ministry's representations, and I find that although the Ministry is in "possession" of records relating to a court action in a court file,

its limited ability to use, maintain, care for, dispose of and disseminate them does not amount to “custody” for the purposes of the *Act*. Nor do I find, in applying the factors set out in Order 120 to the evidence before me, that there are indicia of “control” over these records by the Ministry.

For these reasons, I find that the Ministry does not have custody or control over records relating to a court action in a court file within the meaning of section 10(1) of the *Act* and, accordingly, to the extent that such records are located in a “court file”, they cannot be subject to an access request under the *Act*.

I am not satisfied, however, that **this conclusion extends to copies of such records which exist independently of the “court file”**. Accordingly, to the extent that copies of these records also exist independently of the “court file”, **they would fall within the custody and/or control of the Ministry and, therefore, would be subject to the *Act*** [emphasis added].

Order P-994 clarifies that where records in the possession of MAG constitute part of a court file, these records are not subject to the provisions of the *Act*. Notwithstanding this fact, Order P-994 also makes clear that copies of official court records that exist **independently** of a court file would be considered to be under the control or custody of the institution, and therefore subject to the provisions of the *Act*. I agree with the analysis in Order P-994 and adopt it for the purposes of my investigation under the *Act*.

In this case, many of the records containing personal information were removed during garbage and recycling pickup, and it was not possible to identify whether the records were “court records” (*i.e.*, official copies of a record being maintained in a court file) or other types of records, or were copies of court records that existed independently of the court file.

As I have indicated above, the sample records that I obtained from my site visit included Notice of Assignment Court, Pre-hearing Conference Report form, Notice of Intention, and Bench Warrant Certificate, among others. Given the fact that the records were separate from the court files at the time they that were picked up, it is likely that most of the records were copies, or were otherwise not part of an official court file and were therefore not “court records”. Consequently, these records would be subject to the *Act*.

Are the records excluded under section 65(5.2) of the provincial *Act* and section 52(2.1) of the municipal *Act*?

Section 65(5.2) of the provincial *Act* states:

This Act does not apply to a record relating to a prosecution if all proceedings in respect of the prosecution have not been completed.

Section 52(2.1) of the municipal *Act* contains wording that is identical to section 65(5.2) of the provincial *Act*.

The impact of this provision is that it excludes any record relating to a prosecution that has not yet concluded from the application of the *Act*, including the application of the privacy provisions of the *Act* [Order PO-2703].

In this case, as stated above, most of the records that are the subject of this investigation cannot be examined. Therefore, it is not possible to determine whether or not these records are, in fact, records relating to a prosecution where the proceedings have not yet concluded.

Given the fact that prosecutions do take place at OCH, it may be reasonable to surmise that some of the records in question may be subject to this exclusion. However, it is not possible to say that **all** of the records set aside for disposal related to prosecutions, and that all proceedings in these prosecutions had concluded.

Because it is not possible to examine the records at issue, I am not able to conclude that the records would be excluded under section 65(5.2) and 52(2.1) of the *Act*. In addition, even if some of the records may be excluded under these two provisions, I also conclude that it is unlikely that all of the records at issue would have been subject to this exclusion.

Further, I would also note that because some of the records may be excluded does not reduce the need to handle them securely. The impact of negligent handling or disposal of excluded records is just as serious as if those records were covered by the *Act*. I assume that Institutions are not taking the position that records containing sensitive personal information may be subject to lax security measures simply because they are excluded from the *Act*. That is a highly technical, and from the public's point of view, unacceptable position.

Is the information “personal information” as defined in section 2(1) of the *Act*?

I will now consider whether the records in question contain personal information.

The records at issue are the records that were viewed by the Global Television news reporter and the records that were collected by the IPC's investigator during the site visit.

The definition of “personal information” is set out in section 2(1) of the provincial *Act* and section 2(1) of the municipal *Act*, 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.

The records picked up on site by the IPC contained individuals' names and a range of other information including court dates, exhibits to be used in court, and arrest warrant information. The content of these records clearly qualifies as personal information.

The records appearing on the Global TV news report had been visually obscured prior to broadcast. However, based on the limited information that was available through a viewing of the broadcast, the records did appear to contain individuals' names, driver's licence numbers and information pertaining to court dates. The content of these records also qualifies as personal information.

All of the institutions involved in this investigation agree with the conclusion that the records contained personal information.

Were the records in question excluded from the application of the privacy provisions of the *Acts* by virtue of section 37 of the provincial *Act* and section 27 of the municipal *Act*?

Part III of the provincial *Act* and Part II of the municipal *Act* are the provisions of the *Acts* that deal with the protection of personal information.

Section 37 of the provincial *Act* states:

This Part does not apply to personal information that is maintained for the purpose of creating a record that is available to the general public.

Section 27 of the municipal *Act* contains wording that is identical to section 37 of the provincial *Act*. Both provisions exclude personal information "that is maintained for the purpose of creating a record that is available to the general public" from the application of the privacy provisions of the *Acts*. These provisions are relevant because some court records are considered to be publicly available records.

The IPC had held that an institution may only claim this exclusion in cases where the personal information is being maintained by institution specifically for the purpose of creating a record that is available to the general public [see for example, MC-980018-1].

In this case, the records at issue are records that were set aside for disposal and most of these records were not available to be viewed. Therefore, it is not possible to conclude that all of the records would have been the sort of records that would have been made available to the general public.

I am therefore satisfied that section 37 of the provincial *Act* and section 27 of the municipal *Act* do not apply to these records.

Based on the above, I conclude that the records are subject to the privacy provisions of the *Acts*.

Furthermore, even if the some of the records were considered to be public records, such a fact should not be seen to relieve an institution of its duty to dispose of such records securely. Court

records are generally made available to the public in order to promote transparency in the justice system. Any potential suggestion that the public availability of these records entails that there is an absence of an obligation of secure disposal would be, in my view, an unacceptable and overly technical interpretation of this provision of the *Acts*.

Was the disposal of the “personal information” in accordance with the provisions of the *Act*?

Having determined that the privacy provisions of the *Acts* apply to the records, it is necessary to determine whether the disposal of the records was in accordance with the *Acts*.

There are various provisions, in both the provincial *Act* and municipal *Act*, as well as the Regulations made pursuant to those *Acts* that address the disposal requirements for records containing personal information.

Section 40(4) of the provincial *Act* states:

A head shall dispose of personal information under the control of the institution in accordance with the regulations.

Section 30(4) of the municipal *Act* contains a provision that is equivalent to section 40(4) of the provincial *Act*.

Regulation 459, made under the provincial *Act* is titled “Disposal of Personal Information”, and deals exclusively with the manner in which provincial institutions are required to dispose of records containing personal information.

Section 4 of Regulation 459 states, in part:

- (1) Every head shall ensure that all reasonable steps are taken to protect the security and confidentiality of personal information that is to be destroyed, including protecting its security and confidentiality during its storage, transportation, handling and destruction.

...

- (3) In determining whether all reasonable steps are taken under subsection (1) or (2), the head shall consider the nature of the personal information to be destroyed or transferred.

...

These regulatory provisions impose a duty on institutions to dispose of personal information in a secure manner, and to be cognizant of the nature and sensitivity of the record at issue when disposing of records containing personal information.

Although there is no Regulation analogous to Regulation 459 under the municipal *Act*, section 3 of Regulation 823, the General Regulation to the municipal *Act* states:

- (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.
- (2) Every head shall ensure that only those individuals who need a record for the performance of their duties shall have access to it.
- (3) Every head shall ensure that reasonable measures to protect the records in his or her institution from inadvertent destruction or damage are defined, documented and put in place, taking into account the nature of the records to be protected.

Section 4 of Regulation 460, the General Regulation to the provincial *Act* contains similar wording and imposes similar requirements on provincial institutions.

Although municipal institutions are not subject to provincial Regulation 459, section 30(4) of the municipal *Act* explicitly states that institutions disposing of records must dispose of those records in accordance with the regulations. Because Regulation 823 **does** apply to municipal institutions, I am satisfied that section 30(4) of the municipal *Act*, read in conjunction with Regulation 823 imposes responsibilities on institutions as follows:

- to have written measures in place to prevent unauthorized access to records during disposal;
- to ensure that access to records set aside for disposal are limited; and
- to ensure that measures put into place be documented and to take into account the nature and sensitivity of the records in question.

In Order HO-001, the IPC addressed the proper destruction and disposal of records of personal health information under the *Personal Health Information Protection Act* (PHIPA). Although PHIPA contains provisions that are different from those in the provincial and municipal *Acts*, both PHIPA and the *Acts* are premised on “fair information practices,” which are internationally recognized principles dealing with the fair treatment of records containing personal information. Although this investigation is not conducted pursuant to PHIPA, in my view, some of the principles expressed in Order HO-001 are relevant to my analysis in this investigation.

Among other order provisions in Order HO-001, Commissioner Cavoukian made the following order:

I further order the [organization in question] to put into place a written contractual agreement with any agent it retains to dispose of personal health information records. The agreement must set out the obligation for secure disposal and require the agent to provide written confirmation through an attestation once secure disposal has been conducted.

In addition, the IPC's position on information destruction has been expressed in the Fact Sheet titled *Secure Destruction of Personal Information*² (the *Fact Sheet*) which states that all records containing personal information must be destroyed in a secure manner, and includes suggestions respecting contracting with service providers to provide secure destruction services.

As I have indicated previously, each of the four institutions were asked to provide their position with respect to the following points:

1. Whether appropriate records destruction practices are set out in a written policy.
2. Whether the policy has been disseminated to staff, and whether staff have been trained in its application.
3. Whether the physical layout of the program area facilitates the promotion of secure destruction of records containing personal information.
4. In cases where institutions utilize service providers to provide information destruction services, whether the institution has written contracts in place with the service provider including provisions regarding the provider's obligations with respect to destruction.

I will now assess whether the practices of the institutions that are subject to this investigation are in accordance with the *Acts* and the *Regulations* thereto.

Ministry of the Attorney General

MAG provided its position on the issues raised in this complaint both at meetings and in written correspondence to the IPC. MAG also completed an internal investigation into the matter and provided a report to the IPC.

With respect to destruction of records containing personal information, MAG confirmed that all MAG offices at OCH (along with the entire Ministry) are subject to MAG's Policy on Confidential and Personal Information, which mandates that all records containing personal information should be disposed of through shredding. This policy is available for review on MAG's intranet site. MAG advised that locked bins are located throughout the Court Services Division (CSD) offices, where staff are instructed to deposit records containing personal or confidential information. The locked bins are picked up and the contents are shredded by an information destruction company on a bi-weekly basis. In addition, there is a large shredder in one of the CSD offices.

MAG stated that CSD staff involved in the disposal of documents are trained on the proper means of maintaining and disposing of records, and that the general training of all new CSD staff includes a component dealing with the secure destruction of records containing personal information.

² http://www.ipc.on.ca/images/Resources/up-fact_10_e.pdf

MAG also provided information on the information destruction policies of the Criminal Law Division (CLD) and the Victim/Witness Assistance Programs (V/WAP) offices operating at OCH. MAG confirmed that staff within these departments are also trained on secure information destruction. With respect to the CLD, staff are instructed to dispose of all confidential information in secure bins that are provided by a service provider. MAG advised that each staff member at the V/WAP had an individual shredder and was instructed to “shred everything”.

MAG stated that, in response to this privacy investigation, it has introduced additional measures to further enhance and promote the secure destruction of records containing personal information at OCH, including the following measures:

- A “shred-all” policy (*i.e.*, instructing staff to shred *all* documents that are disposed, rather than just confidential records, or records containing personal information) for all MAG program areas operating at OCH, including CSD, CLD and V/WAP.
- Sending a letter to the City requesting that the City cease the practice of placing garbage and recycling on the curb the evening before scheduled pickup times.
- Notifying the Chief Information and Privacy Officer for Ontario as well as the Judiciary about the incident.

MAG responded to the IPC’s questions as follows. With respect to the need for a written policy, MAG confirmed that it does have a ministry-wide policy in place addressing the disposal of records containing personal information. The policy mandates that records containing personal information should be destroyed through shredding. With respect to the dissemination of the policy, MAG has stated that the policy was disseminated to MAG staff through the Ministry’s Intranet website. MAG further advised that staff at OCH who dealt with personal information in the various offices had been trained on the proper means of destroying such records.

With respect to the office layout, the IPC noted the presence of secure bins designated for shredding in the MAG CSD offices. MAG stated that its CLD offices within OCH also have secure bins on site that are used for the secure disposal of records, and that all staff members at the V/WAP offices operating at OCH have their own small shredders.

With respect to agreements with service providers, MAG confirmed that both CLD and CSD have contracts in place with companies providing record destruction services. In both cases, the service providers provide a certificate of destruction once the shredding has been completed. MAG advised that, in response to this investigation, the V/WAP also contracted with a service provider to provide information destruction services.

In addition, in response to the draft Report, MAG also confirmed that Court Services Division has re-issued the memorandum to staff at OCH reminding them of the requirement to securely dispose of confidential records.

Based on the information provided by MAG, I am satisfied that the MAG offices operating at OCH had adequate information destruction measures in place as of the incident. I conclude that MAG's policies and procedures on the disposal of personal information were in accordance with the provincial *Act*.

As discussed above, MAG also conducted its own internal investigation into the incident. As a result of this investigation, MAG has made a number of recommendations for further enhancing its records destruction practices at OCH. I have reviewed MAG's internal recommendations and I agree that the adoption of these recommendations would further improve MAG's information destruction practices at OCH.

City of Toronto

The IPC conducted a site visit and met with City staff. The City provided its position on the issues in this complaint in writing. The City also provided additional information in response to the draft of this Report. The City confirmed that it is the owner of OCH and is responsible for building operations. In addition, the City is also responsible for the operation of three City divisions operating at OCH: the City's Court Services, Legal (Prosecutions Unit), and Facilities.

As part of its responsibilities for building operations, the Facilities Division is responsible for picking up garbage and recycling from the various offices within OCH. The City confirmed that on the day of the incident in question, Facilities staff placed garbage and recycling collected from the building on the curb to await pickup. Further, the City confirmed that, as is customary under the City's waste management protocol, the garbage was placed in clear plastic bags.

With respect to its policies on information destruction, the City provided the IPC with a copy of a policy on the City's intranet titled: "Records and Information Management: Disposal of Records at your location". The policy states, in part:

Maintaining the confidentiality of the Corporation's records is everyone's concern. Records or files should never be discarded directly into a wastebasket. In City Hall and Metro Hall, there are red confidential recycling bins in the photocopying room on every floor. Transitory records or transitory files containing personal or confidential information should be placed inside these red containers.

The City stated that while the confidential waste disposal policy applied to all City facilities, including its offices at OCH, City offices at OCH did not have "adequate access to secure disposal methods in order to implement the policy". Specifically, the City stated that at the time of the incident the red bin program mentioned in the policy was not in place at all City facilities and that City offices at OCH were not part of the City's confidential waste disposal program.

The City stated that it currently has a "No Waste" program in place. Under this program, a desk-side paper recycling bin is placed at each desk location and central recycling bins are also made available. Employees are expected to use the desk-side bins and then transfer the contents into the central bins. A copy of the "No Waste" program page from the City's intranet was provided

to the IPC. The City acknowledges that the “No Waste” intranet page does not mention separating confidential documents from other documents. Further, the City has acknowledged that it has been convenient for staff to place their documents (presumably including records containing personal information) in the general recycling.

The City also provided the IPC with its clean desk policy, which applied to all City staff and states:

At the end of the day, return all documents to the proper filing cabinet or drawer and lock it; use shredding facilities or other confidential means to dispose of unwanted copies; empty your wastebasket; lock your office door.

Based on the above, I note that while the City had policies for secure destruction that applied to its offices at OCH, these offices did not have the proper measures in place to implement the policies. Specifically, the City’s policy was lacking in that the red bin program, including the requisite contract with a service provider, was not in force at the OCH offices at the time of the incident.

With respect to training and dissemination, the City stated that records management training was last provided to court services staff at OCH in 2002, and that the secure destruction of records was a component of this training. The City has also noted that it offers general training programs that are available on a sign-up basis as follows:

- a general training program on privacy protection, including secure information destruction that is offered monthly at the City’s Corporate Learning Centre; and
- a quarterly training program on Records and Information Management, which also includes instructions on secure disposal of confidential records.

While I am pleased that that the City’s Court Services staff had mandatory training on records management in 2002, and the City now offers general privacy and training programs on a sign-up basis, I note that, at the time of the incident, not all City staff at OCH would have been trained in the secure destruction of records. Specifically, those City staff that were employed by the City after 2002 and who had not elected to take the optional courses would not have had such training.

In my view, the orientation of all new staff should include training on the secure destruction of personal information. Because this mandatory training was not a component of staff training at the time of the incident, I am not satisfied that staff training was adequate at that time.

With respect to the third question, (layout) I note that while the City’s Court Services office had a paper shredder on site, there was not a paper shredder in the Prosecutions office. Accordingly, I am not satisfied that the physical layout of this office adequately promoted the secure destruction of records.

With respect to the fourth question, at the time of the incident, the City offices within OCH were not part of the City's confidential waste disposal program, and accordingly, City offices at OCH did not have a contract with a service provider providing information destruction services. The City had stated that it had a contract with an information destruction service provider for its buildings in the secure bin program, but that this contract did not include OCH.

To summarize, this investigation has identified the following shortcomings with respect to the City's information destruction practices at OCH as of May 4, 2007:

- The City did not have proper measures in place at OCH to implement its policies on secure destruction;
- Not all City offices had either a physical paper shredder on site or a secure bin and the City's offices at OCH did not have a contract in place with an information destruction service provider; and
- General staff training on privacy and secure information destruction, particularly with respect to orientation of new employees, was lacking.

Based on the above, I conclude that the City's information destruction practices were not in accordance with section 30(4) of the municipal *Act* and section 3 of Regulation 823 under the municipal *Act*.

In written materials provided to the IPC, the City has acknowledged that its information management practices and policies at the time of the incident were inadequate and may have contributed to the privacy breach. Further, the City has stated that it has taken a number of steps to reduce the risk of a similar incident from occurring in the future.

In the days following the incident, in response to this investigation, the City took the following steps:

- The City temporarily ceased the practice of placing garbage and recycling on the curb on the evening prior to scheduled pickup times.
- The Directors of Court Services and Prosecutions sent written reminders to all staff to dispose of confidential documents and documents containing personal information by shredding or by placing them in the confidential red waste bins.
- Confidential red waste bins were installed throughout all City offices within OCH.

The City has also indicated that it has implemented, or is in the process of implementing the following longer-term steps:

- The City's Corporate Access and Privacy Office, together with the Records and Information Management Office, will be providing privacy and records management training to all City staff at OCH. This training will include safeguards for protecting privacy and the necessity of secure disposal for confidential documents.
- The City's contract with a service provider to provide records destruction services will be expanded to include information destruction services at OCH.
- Signage has been placed at all public garbage areas at OCH indicating that secure disposal of documents is available.
- A Fact Sheet titled *Secure Destruction of Transitory Personal and Confidential Information* has been drafted and will be posted to the intranet for City staff.
- Policies directed to staff regarding the "No Waste" program will be amended to emphasize that confidential documents are not to be disposed of in general recycling containers.
- The City Clerk has sent a memorandum to City senior executives containing strong privacy and secure records destruction recommendations.

I commend the City for acknowledging the shortcomings in its information destruction practices and policies and I am pleased with the steps that have been taken to improve them.

Ministry of Community Safety and Correctional Services

The Probation and Parole (P&P) office at OCH is operated by the MCSCS and has provided its position on the issues raised in this complaint in writing.

The MCSCS policy regarding information destruction is set out in the MCSCS *Probation and Parole Administrative Processes Manual* (the *Manual*), which is published on its intranet site. A copy of the *Manual* has been provided to the IPC. The *Manual* states:

Shred anything with client names or client information rather than place in the garbage.

MCSCS advised that it has prepared a new *Freedom of Information and Privacy Best Practice (Best Practice)* on the topic of record security, retention, and disposal. The *Best Practice* contains specific information on the requirements for secure destruction of records.

With respect to training, MCSCS indicated that orientation for all new staff in the P&P office includes training on applicable legislation, policies, and procedures. Further, MCSCS stated that on June 5, 2007, the Area Manager responsible for the P&P office met with staff to highlight sections of the *Manual* dealing with the requirement to shred records containing personal

information. MCSCS stated that the training for all new staff includes a component on the secure destruction of information.

MCSCS advised that, prior to the incident, records containing personal information, such as court dockets, were stored on shelves in a secure area of the office. Once the shelves became full, a grey bin would be brought into the office, and the records placed in grey bins would be securely disposed of by an information destruction company. (MCSCS informally employed the services of an information destruction company that was under contract with MAG to dispose of materials set aside for destruction within the P&P office).

MCSCS has further stated that in response to incident, the following steps have been taken:

- Permanent grey bins are now maintained within the P&P office at OCH and are removed and securely destroyed once full;
- Recycling bins have been removed from the office; and
- The P&P is considering formalizing the informal agreement in place with the information destruction service provider to securely dispose of information in grey bins.

With respect to the first two questions outlined above, I note that training and orientation is provided to new staff on legislation, policy, and procedures relating to confidentiality. Accordingly, I am satisfied that MCSCS has adequate policies in place and that these policies and procedures are disseminated to all staff.

With respect to the third and fourth questions, MCSCS has stated that the office itself is a controlled access area, with a paper shredder on site. Court dockets are placed on shelving units, and, once the shelves are full, are picked up by an information destruction service provider. MCSCS has stated that it uses an information destruction service provider that is under contract with MAG to provide destruction services.

With respect to the practices in place at the P&P office at the time of the incident, I note the following shortcomings:

- It would be preferable for staff to maintain records set aside for disposal in secure bins, rather than on shelves in the P&P office. Although the P&P office is a restricted access area, the fact that records are exposed gives rise to potential risk; and
- It would be preferable for the P&P office to contract directly with a service provider to provide destruction and disposal services. The fact that the informal arrangement in place with a service provider that is under contract with a different entity (MAG) does not provide that the service provider is contractually obliged, and therefore directly accountable to MCSCS.

Therefore, I am of the view that the MCSCS' information destruction practices were not in accordance with section 40(4) of the provincial *Act*, Regulation 459 under the provincial *Act*, and section 4 of Regulation 460 under the provincial *Act*.

Subsequent to its review of a draft of this Privacy Complaint Report, MCSCS confirmed that the recommendations contained in the draft and set out below had been implemented and that:

- a locked bin provided by a records destruction service has now been placed in the P&P office; and
- MCSCS' existing secure records destruction contract has been extended to include the P&P office at OCH.

I am pleased that MCSCS has been proactive in identifying, and addressing the shortcomings that have been identified as a result of the incident.

Toronto Police Service

The TPS provided its position on the issues raised in this complaint to the IPC in writing. The TPS confirmed that the TPS Unit at OCH does have a policy on the shredding of materials as follows:

...the staff working out of OCH which comprise both court officers and civilian clerks, are cognizant of the policies concerning the destruction and disposal of personal and identifiable records. ... All new staff is trained on the procedure and process of shredding. This policy is readily available on each TPS internal computer directory as well as paper copies in the office

The TPS have provided an excerpt from *Procedure 17-03, Municipal Freedom of Information and Protection of Privacy Act, (Procedure 17-03)* which expresses the requirement to dispose of records containing personal information and states:

When disposing of records containing personal information shall:

- shred the appropriate paper waste by using the unit shredder, where available, or
- deposit the appropriate paper waste into a designated shredding bin.

The TPS advised that its offices at OCH have two locked bins and one shredder. When bins are full, the TPS contacts an information destruction company to pick up the shredded materials. The TPS stated that all new staff are trained on the procedure and process of shredding, and that all staff are cognizant of the policies concerning the destruction and disposal of records containing personal information.

With respect to the four questions outlined above, I note that TPS *Procedure 17-03*, which is excerpted above, requires that staff working in the TPS Unit at OCH securely dispose of all records containing personal information.

With respect to training, as stated above, the TPS has indicated that staff are cognizant of the policies concerning the destruction and disposal of personal and identifiable records and are trained in the procedure and process of shredding.

In terms of office layout, I note that there are two locked bins for shredding within the TPS Unit.

With respect to information destruction services, the TPS has confirmed that it has contracted with a service provider to pick up the materials in the locked bins for disposal, and has confirmed that it is provided with a certificate by the service provider after the completion of each collection.

In light of the above, I am satisfied that the TPS has provided adequate responses to the questions raised in this investigation.

SUMMARY OF KEY STEPS TAKEN TO DATE:

As mentioned above, some of the institutions having offices at OCH have already taken steps to improve information destruction practices at OCH. I commend the TPS for already having appropriate measures in place. I also commend the institutions listed below for the steps taken to date to improve their respective approaches to the secure destruction of records containing personal information. The key steps may be summarized as follows:

Ministry of the Attorney General

- An internal investigation was conducted, which resulted in recommendations being made for further enhancing MAG's records disposal practices.
- Implementing a "Shred-All" policy for all program areas at OCH.
- Memoranda sent to all Divisional directors reminding them of the requirement for the secure disposal of records containing personal information.
- Having the V/WAP office contract with a service provider to provide records destruction services.

City of Toronto

- Memoranda sent by Directors of the City's Court Services and Prosecutions department respectively, reminding all staff to dispose of confidential documents and documents containing personal information by shredding or by placing them in the confidential red waste bins.

- Installation of confidential red waste bins throughout all City offices within OCH.
- Provision of privacy and records management training to all City staff at OCH by the City's Corporate Access and Privacy Office and the Records and Information Management Office.
- Expansion of the City's contracts with service providers to include City offices at OCH.
- Placing signage at all public garbage areas at OCH indicating that secure disposal of documents is available.
- Preparing a Fact Sheet on the secure destruction of transitory personal and confidential information and posting it to the City's intranet to guide City staff.
- Discontinuing the use of desk-side recycling bins.
- Introduction of audits and spot checks of recycling containers picked up at OCH.
- Providing information on record disposal and privacy to all new and temporary staff as part of orientation and training.

Ministry of Community Safety and Correctional Services

- Placement of a locked bin in the P&P office that is intended to be used for secure disposal; and
- Extending MCSCS' existing secure records destruction contract to include the OCH P&P office.

As noted above, MCSCS has already provided our office with confirmation of compliance with the above recommendations.

CONCLUSION:

It is generally accepted that the court system plays an important role in our democratic society. Accordingly, the courts, along with all of the offices associated with the court system must govern themselves in a way that promotes public confidence and trust.

The court system routinely administers large volumes of records containing information of a sensitive nature, including personal information. While some of this information is a matter of public record, some information is confidential and where access is not properly controlled, its

disclosure can lead to, among other things, loss of personal reputation, embarrassment, and identity theft. Consequently, the offices associated with the court system in Ontario must pay close attention to the manner in which they dispose of records containing personal information.

During the course of this investigation, I have assessed whether the records destruction practices and policies of the institutions operating at OCH are in accordance with the applicable provisions of the provincial and municipal *Acts* and the associated regulations. I have identified various shortcomings and I make my recommendations below.

RECOMMENDATIONS:

I make the following recommendations:

City of Toronto

1. Draft a comprehensive policy on records and information destruction that applies to all of the City offices operating at OCH. The policy must provide that all records containing personal information be disposed of in a secure manner.
2. Provide staff training on the policy.
3. Ensure that the orientation of new staff includes training on privacy protection, and specifically, the secure destruction of records.
4. Ensure that either secure bins for destruction or physical papers shredders are located in every City office at OCH that may handle records containing personal information.
5. Ensure that any services received from information destruction service providers are subject to a contract, and that a certificate of destruction is provided by the service provider once destruction has taken place.

By March 12, 2009, the City should provide the IPC with proof of compliance with the above recommendations, or proof that steps to comply are underway.

Original Signed by: _____
Mark Ratner
Investigator

December 12, 2008
