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

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NOS. PC-040019-1, PC-040021-1 and PC-040022-1

Ministry of Health and Long-Term Care

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/Téléc: 416-325-9188
TTY: 416-325-7539
http://www.ipc.on.ca

PRIVACY COMPLAINT REPORT

PRIVACY COMPLAINT NOS. **PC-040019-1; PC-040021-1; PC-040022-1**

INVESTIGATOR: **Alex Kulynych**

INSTITUTION: **Ministry of Health and Long-Term Care**

SUMMARY OF COMPLAINT:

The Office of the Information and Privacy Commissioner/Ontario (the IPC) received complaints under the *Freedom of Information and Protection of Privacy Act* (the *Act*) concerning the Ministry of Health and Long-Term Care from three patients at the Oak Ridge site of the Penetanguishene Mental Health Centre (the Centre). Specifically, the complaints relate to inspections of the patients' computers and related equipment and material and the consents that patients were asked to provide in this regard.

The complainants maintain that the consent they were asked to sign was too broad and was requested, in their view, in a coercive manner such that if consent was not given, access to their computers was revoked. They feel that the impounding and inspection of their computers and related equipment under these circumstances was an inappropriate collection of their personal information and contrary to the *Act*.

In addition, one complainant (PC-040019-1) is also of the view that "spyware" had been installed on his computer during the course of the computer inspections. The same complainant feels that the apparent purpose of the search - to locate pornographic material, including child pornography, and copyright violations - is a criminal matter and the Centre does not have the jurisdiction to investigate criminal offences. He adds this as another reason why the computer searches should not have taken place.

Another complainant (PC-040021-1) is concerned that his CDs, containing personal information, are being stored in the nursing management office and not in a lockbox in his room as is the case with other patients.

BACKGROUND:

The Ministry provided the following background relating to this case.

The Oak Ridge facility at the Mental Health Centre, Penetanguishene, is an all male, maximum-security facility for mentally-disordered offenders most of whom have been found Not Criminally Responsible on account of mental disorder, or Unfit to Stand Trial in relation to serious personal injury offences.

According to the Ministry, in February 2004, the Centre became aware of allegations by a number of patients that a particular patient was in possession of child pornography. With this particular patient's consent, his computer system, including CDs and DVDs, was examined. The examination revealed a highly sophisticated system, capable of, among other things, disguising attributes of files (for example, make movie files look like text files).

Based upon what was discovered, which included various types of pornography, hospital officials reached a number of conclusions. The Ministry explained that it took the following steps:

> These observations and conclusions were presented to hospital senior management who approved funds to proceed immediately with retaining an outside expert to assist with the review of computer security procedures. An expert was contacted and a meeting held February 25, 2004.
>
> …
>
> On February 19, 2004 clients were advised in writing that changes to security procedures regarding client-owned computers would be forthcoming…On February 20, 2004 the Chief of the Forensic Division met with clients to review this issue with them (all clients were invited but few attended) and to present to them a Consent form that they were asked to consider, that would authorize the hospital to search their computer systems and related equipment and material… Clients were advised that providing this consent was voluntary, but that failure to do so may result in removal of their computer systems to inaccessible storage. Clients were given until February 25, 2004 to make their initial decision regarding consent. They were advised that consent could be given or revoked at any time but that access to their computers would be granted or denied consistent with the hospital having the authority to search the computer systems.
>
> There are 140 clients at Oak Ridge. There are approximately 22 clients in Oak Ridge who own computer systems. Some clients own two systems or more. Approximately 8 clients came to the general meeting. Clients were provided with copies of the contraband policy, and a copy of the consent form. There was productive dialogue and several questions raised and answered. The documents were subsequently distributed to all computer owners and to all wards.
>
> …

The Ministry also provided the following information:

> The computers and related equipment and material are owned by the patients. The systems that are inspected by the consultant consist of desk-top and/or portable computers and external mass storage devices (removable hard-drives, disks, DVDs etc).
> …
>
> The systems contained computer files of all types including executable (program) files, text files, data files, video files, audio files and photograph files.

DISCUSSION:

The following issues were identified as arising from the investigation:

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

Section 2(1) of the *Act* states, in part:

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

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

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they relate to another individual,

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual, and

(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;

All three complainants submit that their computers and related equipment and material contain some or all of the following: income tax returns, banking statements, credit card accounts, solicitor-client correspondence and personal letters, including others' names and addresses.

The Ministry acknowledges that some of the information on the complainants' systems at the time of inspection may qualify as "personal information".

I conclude that at least some of the information contained in the complainants' computers and related equipment and material qualifies as "personal information" as defined in section 2(1) of the *Act*.

Did the Centre collect personal information in accordance with section 38(2) of the *Act*?

***Introduction*:**

Section 38(2) of the *Act* sets out the circumstances under which personal information may be collected on behalf of an institution. This section states:

> No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity.

***Representations*:**

In its representations in response to the present complaints, the Ministry provided the following information with respect to the manner in which the Centre's patients' computers have been inspected:

> Files are inspected but not reviewed or read. The inspection process has no interest in text files, but only in files containing images or video. Only large text files are inspected, and then only to ensure that they, in fact, contain text and not other content…
> …
>
> Additionally, the hospital is conducting computer systems inspections in such a manner that client concerns should be obviated. First, the hospital has arranged to have the client-owned computers inspected while the client directly observes the process. Clients may monitor the process either through a window facing the computer monitor being used by the inspector, or in the room with the inspector if other staff are also present. Second, all computer related material and equipment that is not permitted in the clients possession (for example, clients are being permitted 150 discs in their possession but the rest must be placed in storage) is placed in a box provided by the hospital. That box is locked by the hospital and left in the client's possession. The client retains control of it; but is not be able (sic) to access the contents excepting through the inspection process. Third, a

client who declines to authorize the hospital inspection of his computer systems has two choices. If he authorizes the hospital to do so, the hospital will disable the client's computer system (by pulling a plug to the power supply), apply security seals to the box, and leave the computer in the client's possession. If the client refuses to provide that authorization the hospital will be obliged to physically remove the client's computer system to hospital storage.

…

The [named] consultant's inspection process consists of the following;

A. The inspection does not begin until the client joins us in the private office or waives their right to be present. The curtain is placed over the window to afford privacy to the client and the data that will appear on the computer screen. The client can opt to have the window left uncovered if they wish.
B. The computer system (tower, desktop case or laptop) is hooked up to a hospital-supplied monitor, keyboard, mouse and power cord. Any additional storage devices (USB hard discs etc) that may accompany the client computer are also readied for insertion upon completion of the drives presently in the computer system.
C. The machine is booted. The operating system should load and the procedure begins. If through device failure or for other reasons, the system fails to boot then technical assistance is offered. This may include the booting of the system from a provided bootable CD-ROM with an alternative operating system on it, which does not require that the client's computer to be properly configured with an operating system. (IE: damaged install of Windows or LINUX)
D. If this is the first-ever check of the system, a simple auditing utility is installed. This utility is FREEWARE called Belarc Advisor v.6.1f. The utility enumerates the system and the registry and outputs the results to a HTML file which is displayed on the client's computer. The data includes the system components, configuration settings, software listings and serial numbers to provide a baseline configuration report to the hospital of the computer at the time of first inspection.
E. If the client's computer does not recognize the hospital-provided HP Deskjet 895Cxi printer, then the necessary driver is installed to facilitate the printing of this report. A second copy of the printed output is offered to the client.
F. The Belarc Advisor software is uninstalled and no files or data are left behind.
G. The next step is to examine the contents of the computer's hard disc(s) and sort files by type (images, movie clips, movie files and hard disc images such as those created by applications such as Norton Ghost or the like). Those files are viewed in a suitable viewer provided by the operating system. In systems where there are hundreds of qualifying files located across several hard discs or removable drives, another utility is installed to expedite the cataloguing and reviewing of these file types. SHAREWARE

utility CD Vista v.1.10 is installed and instructed to search, report and organize qualifying files for fast and easy review. During this process a single database file is created on the client's computer.

H. After reviewing the data, CD Vista is uninstalled. The database file is left behind. The database file is in a proprietary format and cannot be easily viewed in any other applications. It does not contain executable code or instructions and could just as easily be manually deleted after each search.

I. The next step is to scan the drives for signs of compressed or hidden archives that could contain a collection of prohibited material. Efforts are made to discover hidden, modified or altered files and folders that could hold clandestine content. Basic scans are made to uncover encrypted volume files, which could also be a hidden repository. This is the most time consuming part of the search.

J. Finally, a search is performed to reveal recently deleted data on the hard discs. This search is critical as clients could simply delete a file to avoid detection and recover it from its deleted state after the inspection. If, upon examining the deleted data, suspect material is found, it could be optionally restored to confirm its status or the client could opt to have all slack drive space (empty or marked as being available for new data) erased. This process can be lengthy as it overwrites the effected sectors with seven passes of random data rendering the old data completely unrecoverable. A FREEWARE utility called Restoration v.2.5.14 is used for this purpose. This utility is loaded into RAM and is not installed on the client's computer. No traces of this application are left behind.

K. As a final step, another FREEWARE utility called Eraser v.5.3 is offered to the client, which allows him to completely erase data that they thought they had deleted. Using this application reduces the time spent on having their computer searched and may offer peace of mind that data that they deleted from their machines, possibly to ensure their compliance with hospital policy, is not inadvertently discovered on their machines during a search.

L. It should be noted that at no time, is any software installed on the client's computer without their knowledge and consent. The process, should they choose to stay in the room, is open, transparent and explanations are freely provided along the way. Every keystroke and mouse click is under the scrutiny of both the client and the supervising staff member(s). The client can withdraw their consent to the search at any time in which case the search is halted and the computer system is placed in inaccessible storage.

M. Once a hardware search is completed, a search begins on all removable media (CD-ROM/CD-R/CD-RW/DVD-ROM/DVD-R/DVD-RW and floppy discs) provided with the computer or removed from personal storage boxes. The media is viewed on the client's computer. Media that is mass-manufactured or of the read-only nature can, at the consent of the client, be stamped with a thermal transfer film showing its status as 'Approved'. CD media with this label on the inner ring are exempt from

> future searches, speeding the process up for both the hospital and the client, allowing them easy future access to this media.
>
> …
>
> Inspections are designed to detect files that are most likely to contain contraband and these files are inspected for contraband. Information that is not contraband is not examined. The files are inspected by the consultant and/or assigned hospital staff.
>
> …
>
> No information contained on the computers or related equipment and material was copied or recorded.
>
> …
>
> No information was collected. Where contraband was discovered upon inspection either the contraband was deleted or the computer/equipment/material was placed in storage, at the client's discretion.

***Analysis*:**

Investigation Report I93-044M, involving a municipal licensing commission, addressed the issue of collection under section 28(2) of the *Municipal Freedom of Information and Protection of Privacy Act* (the equivalent to section 38(2) of the *Act*) and whether a collection actually took place in the circumstances of that case. One of the concerns expressed by the complainant, a taxicab driver, was that the licensing commission collected drivers' "trip sheet" records (forms completed by taxicab drivers as they progress through their driving shift) contrary to that Act. According to the complainant, drivers on shift may be stopped by a Licensing Enforcement Officer at any time and be required to allow inspection of their trip sheets.

In discussing whether inspections of taxi drivers' trip sheets by Licensing Enforcement Officers constituted a "collection" under section 28(2), the Information and Privacy Commissioner of Ontario, Ann Cavoukian, Assistant Commissioner at the time, concluded:

> It is our view that the Commission's **inspections** of trip sheets **do not qualify as collections of personal information** within the meaning of the *Act*. In order for a collection to take place, retention of the information in a recorded form must occur. Therefore, in our view, section 28(2) of the *Act* does not apply to the inspection of personal information on trip sheets because collection of personal information in recorded form does not take place. However, it is our view that section 28(2) applies when the trip sheets themselves are retained by the Commission, or when personal information from trip sheets is recorded by the Commission…
>
> …

> Our interpretation has evolved over time, and has been applicable to both appeals and privacy complaints. It is our view that in order for information to be "collected", it must be physically recorded and retained in some manner, other than in an individual's mind. Otherwise, it could not meet the definition of "personal information" within the meaning of the *Act* (ie. **recorded** information about an identifiable individual), nor could it logically be said to be "held" by an institution, or be accessed by the individual. Therefore, we remain of the view that inspections of trip sheets do not qualify as collections within the meaning of the *Act*. [emphasis in the original]

I agree with the Commissioner's comments.

In the current case, before assessing whether the information at issue was properly collected as set out in section 38(2) of the *Act*, I must determine whether a collection, within the meaning of the *Act*, actually took place. In order to do this, I will consider the criteria for collection as outlined above.

The complainants' computers and related equipment and material, as well as the personal information contained therein, are the complainants' property. They are owned by the complainants, not the Ministry. The complainants created or collected the personal information for their own use, not for use by the Ministry. This point is not contested by the Ministry.

However, according to the Ministry's representations, this information was inspected, but was not recorded or copied by the Ministry or placed in the Ministry's files. No contrary information has been provided that would lead me to conclude that the Ministry retained personal information.

In my view, the information at issue was not collected by the Ministry, as envisioned in section 38 of the *Act*. The Ministry did not compile, gather, file, save or otherwise retain the information in recorded form as part of its own records. As stated by the Ministry, where contraband material was discovered, it was deleted or the computer or material was placed in storage. The Ministry did not take possession of the material and therefore cannot be said to have retained the complainants' personal information.

Other Issues:

As previously mentioned, the complainant in PC-040019-1 expressed the concern that "spyware" had been installed in his computer during the course of the inspections. The Ministry has provided a detailed description of the inspection process, including the software programs involved, which has been outlined above.

I see nothing in the information provided by the Ministry to cause me to conclude that the software programs used to conduct the searches of the complainants' computers and related equipment could be considered "spyware". It does not appear that there are elements of any of these programs that monitor usage or collect in a covert manner any sort of data about the computer on which they are loaded.

The only program among them that appears to have the capability of copying and storing data is CD Vista. According to the description of the search process, this program is used to create a

catalogue of the files on a computer and is used to view the contents of the catalogued files. As part of the cataloguing process, the CD Vista program creates a database file in a proprietary format (that is, no other program but CD Vista can read it), which, according to the description of the search process, was left on each of the computers that was searched. It is simply a catalogue, or index, of all the files on the computer. According to the Ministry, this file was left on the computer so that any subsequent searches, if necessary, would be made easier and faster. The file can easily be manually deleted after each search**.** The fact that CD Vista is capable of copying and storing data does not mean that it was actually used for that purpose. As mentioned above, the Ministry has stated that no information was copied or recorded.

The Ministry has recently advised that the CD Vista program has been replaced with a new program called Pictuate to assist in system inspections. The Ministry explains that this new program is not installed on the patient's computer system, but runs from a CD owned by the hospital. According to the Ministry, when the inspection is complete, no files or residuals of any kind are left behind in the patient's system by this program.

Based on the information provided, both initially and more recently, I have no reason to believe that "spyware" was installed during the computer inspection process.

In addition, the complainant in PC-040021-1 is concerned that his CDs have been stored in the Ward Nurse Manager's office and not in a lockbox in his room as is the case with other patients.

In this regard, the Ministry states:

> The client's computer systems and related equipment and materials were removed from his possession and placed in secure storage (some in the Ward Nurse Manager's office and some in his own room in a locked box) when PC-040021 complainant declined to consent to inspection of his system and when he further declined to have his system disabled such that he could continue to have all components left in his possession but inoperable to him.
> …
>
> Due to the amount of computers and related equipment and material, some was stored in a locked box left in PC-040021 complainant's possession, and some was placed in the locked Ward Nurse Manager's office.
> …
>
> Other patients' computers and related equipment were not stored in the Ward Nurse Manager's office. However, all other patients either consented to the inspection of their computer systems and related equipment and material, or consented to the disabling of their computer systems such that the hospital then allowed their systems and related equipment and material to remain in their possession. PC-040021 complainant did neither.

According to the information provided by the Ministry, if an inspection takes place and no contraband is found, the computer and related equipment is returned to the patient. If a patient

does not consent to the inspection, his computer system items are placed in a storage box, locked and placed in his possession in his room. The exception is the complainant in PC-040021-1 whose computer equipment and related material was stored in this manner, but unlike others, his CDs were also stored in the Ward Nurse Manager's office. The Ministry has explained that his CDs were stored in a separate location because this complainant did not consent to either the inspection or the disabling of his computer system and related equipment and material. The separate storage was also due to the amount of computer equipment in his possession. According to the Ministry, subsequent to this complainant's initial refusal to endorse the consent form, he has done so, observed the inspection of his computer system and he is, once again, in possession of that system.

With respect to the concerns expressed by this complainant regarding the storage of his CDs in a location other than in his room, I conclude that this storage was also not a collection under the *Act* for reasons similar to those outlined above. The Ministry did not record or copy this information, nor did it retain the information as part of its records. Accordingly, in my view, the Ministry did not collect this information within the meaning of section 38 of the *Act*.

Other Matters:

Because of the conclusions I have reached with respect to whether the Ministry collected the complainants' personal information, I will not address the portion of the complaints relating to the circumstances surrounding the consent they were asked to sign to allow for inspections of their computers and related equipment. I will also not consider whether the Ministry, even without consent, has the authority to collect personal information in this fashion in the course of the proper administration of a lawfully authorized activity.

I will also not consider whether or not the Ministry's searches for pornographic material or other material is a criminal matter and not within the Ministry's jurisdiction, as argued by one of the complainants. The issue in this investigation is whether the Ministry complied with the privacy provisions of the *Act*. The matter of the Ministry's jurisdiction under other statutes falls outside of the parameters of this investigation and I will not address it in this report.

CONCLUSIONS:

I have reached the following conclusions based on the results of my investigations:

1. The complainants' computers and related equipment and material contain "personal information" as defined in section 2(1) of the *Act*;

2. The Ministry did not collect the complainants' "personal information" under the *Act*.

Original Signed by: September 7, 2005

Alex Kulynych
Investigator