

**ALBERTA
INFORMATION AND PRIVACY COMMISSIONER**

Report of an Investigation into the Security of Personal Information

January 24, 2006

The Business Depot Ltd. (Operating as Staples Business Depot)

Investigation Report P2006-IR-001

I. INTRODUCTION

[1] On May 17, 2005, the Office of the Information and Privacy Commissioner (“the Commissioner”) received a complaint that a Staples Business Depot store in Calgary sold a computer to a customer that contained a previous customer’s personal information (the complainant). The complainant alleged that The Business Depot Ltd. (“Staples” or “the Organization”) disclosed her information without her knowledge and consent and failed to safeguard her information in contravention of the *Personal Information Protection Act* (“PIPA” or “the Act”).

II. JURISDICTION

[2] PIPA applies to provincially-regulated organizations in Alberta. The Commissioner has jurisdiction in this case because Staples is an “organization” according to section 1(i) of the Act.

[3] In conducting my investigation, I met with the complainant (“Ms. A”), and met with “Mr. and Mrs. B”, (the individuals who purchased a computer containing Ms. A’s personal information). I consulted and corresponded with the Organization regarding their policies and procedures. I also received and reviewed sales receipts and computer service records from the individual customers. I collected the serial numbers from the component parts of Ms. A and Mr. and Mrs. B’s computers. At the request of the Organization, I presented this evidence in a meeting between all the parties.

[4] I also engaged the services of an Information Security Technology

firm, Onward Computer Systems, to review the computer and provide a forensic timeline of all technical and software changes to the computer.

[5] The following “Statement of Fact” is agreed by the parties.

III. STATEMENTS OF FACT

[6] On August 3, 2004, Ms. A purchased a computer at a Staples store located at 4307-130th Avenue S.E. Calgary. She was advised that it was a demonstration model but that it had not been used by another customer. However, once she connected the computer at home, she discovered that the hard drive contained another customer’s personal information (Mr. “C”). Ms. A was very concerned about this breach of privacy, and contacted Mr. C to advise him what had occurred. Ms. A then contacted Staples and returned the computer to the store on August 14, 2004. She advised the store about the situation and received a replacement computer. Staples then called Mr. C (a regular customer) to advise him of the existence of the data. Staples reported that they took no further action because Mr. C was not concerned about the disclosure of his personal information.

[7] Ms. A loaded software and personal data on the second (replacement) computer. Subsequently, she was unable to power it up. Because of these technical problems with the second computer, she returned it to the store. Ms. A was told by the store’s technical staff that it was not repairable. The staff told her that her personal data could not be recovered; therefore, it would not be at risk of unauthorized disclosure. Ms. A had a recent back up of her personal information, and was satisfied with the store’s reassurances about the security of the data. She returned the box and software purchased with the second computer. Ms. A was then provided with a third computer. She has experienced no problems with the third computer.

[8] In late April 2005, Ms. A received a call from Mr. and Mrs. B who had purchased a computer from the same store in SE Calgary. They informed Ms. A that their new computer contained her personal information.

[9] Mr. and Mrs. B purchased a computer from Staples on December 21, 2004. Mr. B alleges that he requested a new computer. However, when he turned on the computer in his home, a blank screen with technical text was displayed that discussed system restoration, rather than the normal Window Splash Screen, followed by computer login. Mr. and Mrs. B stated that they did not receive installation or software CDs, as is customary when purchasing a new computer (including the

Operating System reinstallation CDs). Note that Staples stated that the purchase price for the B's computer was below the list price for that model, indicating that it was a returned item or demo model.

[10] Mr. B contacted Staples to attend to these technical difficulties. The Staples technician who came to their home to service the computer found a Staples installation CD in the CD-ROM drive, and the cause of the erroneous screen was deemed to be an internal cable connection problem. After minor adjustments, the computer started up correctly.

[11] When asked about the Staples installation CD, the technician explained that he did not know why it was present in the drive, and that it was an internal CD – not intended for public use. The technician retained the CD. When the technician restarted the computer, Mr. B noticed that the computer operating system was registered to Ms. A. Although the technician observed that this operating system was registered to another person, he took no corrective action.

[12] Installation CDs generally are provided with new computers. Since Mr. and Mrs. B did not receive these CD's, it suggests that the CDs were opened by the previous owner of the computer. This is indicative of the history of the computer.

[13] Within a few days of operating the computer Mrs. B noticed that the hard drive contained many folders and files containing references to Ms. A and her family. The files were of a personal nature, including income tax return information, social insurance numbers, family photographs and employment resume information. The tax files were in the proprietary formats of several retail tax programs, all of which were still installed on the computer, allowing the files to be accessible to Ms. B. Mrs. B used information from the resumes to contact Ms. A to discuss the situation because she was very alarmed about the breach of privacy.

[14] Mr. and Mrs. B did not contact Staples store management to advise them of the discovery of Ms. A's information. Ms. A advised them that she would be taking the complaint forward. Ms. A contacted Staples by telephone on April 27, 2005, and by mail on May 20, and by email on June 20, 2005. In her latter communication, Ms. A indicated that she was unsatisfied with the company's response and advised Staples that any further contact would be through this Office, or through her solicitor. Ms. A did not release the identity of the B's to Staples because she did not have their consent to do so.

[15] Staples does not track serial numbers of computers sold or returned; they advised that it was not a common industry process to retain this kind of information in their sales records. Therefore, I was unable to

compare the serial numbers of the computers through the store's records. Ms. A had registered her second computer with Hewlett Packard on August 16, 2004. She contacted Hewlett Packard during this investigation and provided the serial number to me. This serial number was the same as the hard drive I recorded from the computer in the possession of Mr. and Mrs. B.

[16] During this investigation, Staples was able to track the location of the first computer purchased and returned by Ms. A (the computer containing Mr. C's information). Store management identified the type of computer originally purchased by Ms. A and tracked it through credit card purchases occurring at that time. Staples has not contacted this computer's new owner to confirm whether or not the computer contains any of Ms. A's personal information.

IV. ISSUES

[17] This case concerns the security of personal information on a personal computer. I must determine if Staples failed to make reasonable security arrangements to protect personal information in its custody or under its control.

V. ANALYSIS

[18] Did Staples make reasonable security arrangements to protect personal information in its custody or under its control? Did Staples disclose Ms A's personal information without her knowledge or consent?

[19] Ms. A alleged that her personal information (and that of her family members) was disclosed to unauthorized persons due to Staples' failure to properly erase the data from the hard drive of a personal computer returned to the store.

Section 34 of PIPA states:

An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

[20] It is established and agreed by the parties that Ms. A's personal information was on the returned computer and therefore in the possession of Staples. Staples failed to protect Ms. A's personal information; Staples agreed that it also failed to protect the personal information of the customer whose data appeared on the first computer

purchased by Ms. A. In failing to protect the information, it was disclosed to unauthorized individuals, (Mr and Ms B) without Ms A's knowledge or consent.

[21] Ms. A had no way of removing her personal information from the second computer because it was malfunctioning when she returned it to Staples. She was unable to delete it because she could not power it up.

[22] Mr. and Mrs. B needed no special software to view Ms. A's personal information. The individual files that contained sensitive personal information could be easily viewed simply by navigating to the My Documents folder, selecting a subfolder and double clicking on the file.

[23] Staples agree that this should not have happened. They reported to me that their usual practice is to run a simple system "restore" process on the computers that have been returned by a customer. A "restore" process will delete some of the files, but other files stored on the hard drive will still be accessible. A basic *restore* process will bring the computer back to factory settings and software. For Hewlett Packard computers, the simple restore process is called a "non destructive recovery".

[24] Staples' explanation in the case of Ms. A's returned computer is that since it was not possible to power up the computer, it may have been sent to the Technical Depot (a facility separate from the store). The technical depot is a behind-the-scenes operation that is responsible for repairing computers. This computer was repaired and sent back to the store.

[25] My findings show and Staples agrees that store personnel did not make any attempt to remove or purge personal information belonging to Ms. A before the computer was sold to Mr. and Mrs. B. The store technicians did not even attempt to reformat the hard drive on this computer.

[26] Although Staples reported that the usual process is to reformat the hard drives of computers that have been returned to the store, there is no written policy or procedure or employee training program which directs employees how a defective computer should be received and what steps must be taken by the technicians in identifying whether or not a defective computer's hard drive contains customer data. In addition there are no policies and procedures to remove customer data before reselling this computer or returning it to the manufacturer. The operational staff advised me that the practice is determined by the store managers. Staples often re-sells computers that have been returned within the 14 day return policy. Customers may return computers for

various reasons: they may have minor hardware or software problems, or be defective in some way. Some customers return computers simply because they change their minds about the purchase; many of these customers may not have even powered up the computer.

[27] This Office has no issue or comment about computers that do not contain personal information. However, when a customer returns a defective computer, or advises that he or she has used the computer, I find that running a basic “*restore*” process does not meet the standard required in section 34 of the *Personal Information Protection Act*.

[28] Onward Computer Systems and other industry experts advised me that the destruction of data on the hard drive is the process of overwriting or obliterating data on the hard drives so that the data is useless, unreadable and/or difficult to recover. The destruction or sanitization method must ensure that the data is not accessible to unauthorized users. The extent to which the destruction process is implemented can make it almost impossible to recover any data whatsoever.

[29] Such destruction requires a “*wipe and restore*” process that formats the hard drive on a personal computer. This action will delete all the information on the hard drive and reinstall the original software that came with the computer. Only a “*wipe and restore*” process will overwrite the drive belonging to the personal computer before reinstalling original system files and programs.

[30] In contrast, performing a simple “*restore*” process (Staples’ usual process) replaces system files and original software with the files that originally came with the computer. This process may move or remove certain files, like those stored in “My Documents”. But it is not sufficient to remove all files from the hard drive.

[31] I consulted with industry experts about the time and resources involved in a “*wipe and restore*” process and compared with the simple “*restore*” procedures. The estimates I received were also reviewed by Staples, who agreed with their accuracy. Performing a *wipe and restore* of the hard drive of a personal computer can be done by using the manufacturer’s setup disks. These disks are usually shipped with the computer¹. The total elapsed time from start to finish in such a *wipe and restore* process is two hours; only 20-30 minutes of that time involves active attendance by the technician. An additional 15 minutes of technicians’ time would be required to complete checklists and to

¹ For older systems, obtaining these replacement discs may cost an additional \$12-\$15.

repack the computer into its original boxes. At an average hourly rate of \$20 per hour, it would cost the store approximately \$15.00 in actual staff time to run the process on a computer containing data on the hard drive.

[32] In comparison, running the basic “*restore*” process takes approximately one hour and involves 15-20 minutes of active technician time. In this process, 15 minutes would still be required to complete the checklists and repackage the computer. The net difference in technician staff time between the two processes is 10 minutes, or approximately \$4. I believe this is a very minimal investment to protect the privacy and confidentiality of their customers.

[33] The Privacy Commissioner of Canada received a similar complaint under the *Personal Information Protection and Electronic Documents Act*. This case involved a complainant who brought her laptop into a store where she purchased it for repair. The computer was resold to another customer with the first customer’s personal information on the hard drive. This case was resolved when the store agreed to implement a number of significant changes to safeguard customers’ personal information, including ensuring that it completely wipes customer information on any computer hard drive or other technical device returned to any of its stores across Canada.²

[34] Our office also investigated a similar complaint under the *Health Information Act* in 2003. In this case a faulty computer used by a medical clinic’s transcriptionist re-entered the marketplace when a store failed to destroy the hard drive. The hard drive contained extensive health information of approximately 200 of the clinic’s patients. In this case, the investigator required the clinic and its contractors to ensure that data storage components (hard drives etc.) containing health information be destroyed, or that the health information be permanently deleted through the use of a commercial disk wiping utility.³ The requirements for wiping the hard drives in both of these recent cases are consistent with the *wipe and restore* process outlined in this report.

[35] Staples contravened the Act by failing to safeguard the personal records on the hard drive returned by Ms. A thereby disclosing personal information to unauthorized individuals. Operations staff reported to me

² PIPEDA Settled Case #1: published 2004-11-24 http://www.privcom.gc.ca/ser/2004/s_040623_e.asp

³ Office of the Information and Privacy Commissioner of Alberta, Investigation Report #H0252, June 23, 2004 <http://www.oipc.ab.ca/ims/client/upload/H2003IR002.pdf>

that there have been other incidents of this nature. Even Ms. A had the experience of accessing another individual's personal information on the first computer that she purchased from the store. This is not an isolated incident and I find that the Organization must change its policies and procedures to implement safeguards to mitigate the risk of future privacy breaches.

[36] Staples had opportunities to implement new measures to protect the privacy and confidentiality of their customers when these issues were raised. There were at least two privacy breaches in one store, involving Mr. C's data and Ms. A's data. The technician who attended to Mr. and Mrs. B's computer realized that the computer operating system was registered to another individual. There is no evidence that he even raised the issue with store management. Although Staples knows the identity of the new owner of Ms. A's first (returned) computer, they did not attempt to contact that individual. They have not attempted to confirm whether or not Ms. A's computers were owned by individuals other than Mr. and Mrs. B. I find that Staples should take steps to address these particular breaches, as well as implement policy and procedural changes to address customer confidentiality and privacy issues.

VI. RECOMMENDATIONS

[37] That Staples provide a one-year credit watch service for Ms. A and her affected adult family members.

[38] That the hard drive from the second computer be permanently destroyed once this investigation and review is complete.

[39] That Staples contact the owner of the original computer purchased by Ms. A, and attempt to ensure that any of Ms. A's personal or family information is permanently erased, and confirm this fact to this Office by January 30, 2006.

[40] That Staples track the ownership of the two computers owned by Ms. A and provide confirmation that the computers have not been in the hands of any other third parties by January 30, 2006.

[41] That if other similar complaints are brought to the attention of Staples or to this Office, that Staples provide the same tracking, wiping and notification to that customer(s) that was required in this case.

[42] That Staples must ensure that a full wiping of the hard drive (*wipe and restore* process) is completed on all computers that are returned

either in non-working order, or on computers that contain customers' data on the hard drive.

[43] That if Staples wishes to re-sell computers or components, it should track components by serial number to be able to corroborate the computer hard drives with the erasure procedures.

[44] That Staples include a checklist noting that repair work has been completed and a confirmation that a wipe and restore process has been run on the hard drive.

[45] Staples has agreed to implement the following detailed procedures for all of its retail stores **across Canada**:

- A wipe and restore procedure on any returned computer that is inoperable or that is not certified in writing by the customer to have no personal, confidential or sensitive information stored thereon
- A detailed checklist and technician sign-offs for returned computers
- Introduction of its new policies and procedures as a priority matter and in a prominent way at its forthcoming conference of store managers
- A requirement that store general managers and technicians certify in writing that they have received and understood the new procedures
- Ongoing training on privacy issues, including the new procedures, for all managers and technicians

VII. CONCLUSION

[46] I conclude that Staples contravened the *Personal Information Protection Act* by failing to safeguard personal information in its custody. This failure resulted in the disclosure of personal information to unauthorized persons.

[47] Staples agreed to implement the above recommendation across all stores in Canada to reduce the risk of similar occurrences.

[48] This case illustrates the risks faced by the computer retail industry and serves as a reminder to the industry to be diligent in their practices. These organizations need to factor in the risk to privacy and security in their methods when reformatting and wiping hard drives. Responsibilities under the *Personal Information Protection Act*, the *Personal Information Protection and Electronic Documents Act* and similar laws across Canada require organizations to ensure that their practices and measures are compliant with the safeguarding obligations under the Act.

VIII. COMMENTS

[49] The third parties in this case, Mr and Mrs. B (the individuals who received Ms. A's personal information on their computer), put in a great deal of time and effort providing assistance with this investigation. I thank them for their extensive cooperation and patience with this investigation.

[50] This file is now closed.

Submitted by:

Elizabeth Denham, Director
Personal Information Protection Act
Office of the Information and Privacy Commissioner of Alberta