



Office of the Information and
Privacy Commissioner of Alberta

February 25, 2015

Ms. Liz Kiss, Privacy Officer
Ernst & Young LLP
Box 251
222 Bay Street
Toronto, Ontario M5K 1J7

Mr. Mark Morris (via email & regular mail)
c/o 105 - 2411 4th Street NW
Calgary, Alberta T2M 2Z8

Dear Ms. Kiss and Mr. Morris:

Re: Privacy Complaint File P2685

Mr. Morris (the "Complainant") complained to this office that Ernst & Young LLP (the "Organization", "EY") disclosed personal information, in contravention of the *Personal Information Protection Act* (PIPA), when it sold him decommissioned computer servers.

I have completed my investigation and my findings follow.

The Complaint

The Complainant indicated that on or around August 2006 he purchased two servers from the Organization in Calgary, Alberta. According to the Complainant, he sold one of the servers to a Calgary-area law firm and kept the other in storage. The remaining server stayed in storage until mid-March 2014 when the Complainant had a need for it and powered it up to determine its hardware configuration. According to the Complainant, when he started the server it booted into an operating system. He reset the password and noticed that the server contained numerous files. Based on the file names, he believed that they contained either business or personal information related to the Organization and/or its clients and employees.

The Complainant indicated that he contacted the Organization to alert it to the information on the server. The Complainant exchanged emails with staff from the Organization. The email exchanges between the Organization and the Complainant did not resolve the issue. The Complainant then contacted this office regarding the matter.

Issues

Based on the particulars of the complaint, the issues I investigated were:

- **Issue 1:** Did the server/s contain personal information, as defined in section 1(1)(k) of PIPA?
- **Issue 2:** If the server/s contained personal information, was the information in the custody or under the control of the Organization?
- **Issue 3:** If the server/s contained personal information, did the Organization disclose personal information in contravention of PIPA?
- **Issue 4:** If the servers contained personal information, did the Organization meet its duty to protect the personal information, under section 34 of PIPA?

Background

Previous relationship with the Complainant

According to the Organization, the Complainant worked for Synergy Partners ("Synergy") in Calgary, Alberta as an independent Information Technology ("IT") consultant. Part of his duties included taking care of Synergy's computer servers. On June 2, 2003, EY acquired Synergy.

The Complainant claims that on or around August 2006 the Organization sold him two servers ("Server 1" and "Server 2") that had been used by Synergy.¹ The Complainant claims to have paid about \$300 total. The Complainant was unable to provide the Organization, or this office, with proof, such as a bill of sale or invoice. However, the Organization did corroborate that the Complainant likely did purchase one or more servers from EY.

The recovery of the Servers

It took several months of negotiations between the Organization and the Complainant before the Organization was able to gain access to the Servers.

In July 2014, the Organization commenced legal action against the Complainant. The Organization filed a Statement of Claim with the Alberta Court of Queen's Bench in Calgary on July 18, 2014. The Statement of Claim was accompanied by an affidavit, sworn by the Organization's Privacy Officer, describing the interactions with the

¹ The Complainant presently operates a used computer hardware business.

Complainant, to date, and their efforts to attempt to recover, or get access to, the servers. The Statement of Claim set out a number of remedies sought by the Organization, including a court order allowing the Organization to seize the servers.

On July 28, 2014, the Organization entered into a Consent Order with the Complainant. According to the terms of the Consent Order, the Complainant agreed to confirm, in writing, that the data was secure and that the Complainant had sole custody of Server 1. The Complainant also agreed to arrange for access to Server 1 and provide the name of the law firm in possession of Server 2.

The Organization stated that it sent forensic IT staff to assess Server 1. The IT staff wiped Server 1 of data after taking an image of it. They also inspected 37 other devices that the Complainant had identified as also containing EY data and wiped those devices of information. Nine of the devices contained either full or partial copies of the data from Server 1.

As there was some suggestion that data may be on other devices (e.g., hard drives) held by the Complainant, on December 4, 2014, the Organization and Complainant entered into a second Consent Order. The Order requires that the Complainant ensure any remaining devices that may contain EY data are held in a secure way and to refrain from using, disclosing, copying or reproducing any EY data.

With regard to Server 2, the Organization was able to reacquire the server from the law firm. The Organization also learned that another server was sold to the law firm by the Complainant ("Server 3").

Findings

My findings are based on the submission provided to me by the Organization, as well as information provided by the Complainant.

Issue 1: *Did the server/s contain personal information, as defined in section 1(1)(k) of PIPA?*

Section 1(1)(k) of PIPA defines *personal information* as "information about an identifiable individual."

Initially, the Organization lacked evidence to verify whether EY data, including personal information, was actually on either server.

The Complainant provided this office with a redacted screen capture that appeared to be an Excel spreadsheet of employee-related information. He also provided a copy of a resume that he claimed was one of the many files on Server 1. The resume did not

appear to belong to a current or former employee or the Organization, so it was not clear, on the face of the record, whether it belonged to the Organization. The screen capture of the Excel spreadsheet was also not definitive.

Once the Organization was able to access the data stored on Server 1, it was able to determine that it did, in fact, contain many documents and files. According to the Organization, most of the documents contained information that was not about identifiable individuals. However, some of the documents – approximately 494 – contained information about former partners and employees of Synergy, including names, salary information, SINs and date of birth. This information is considered personal information subject to PIPA.

Based on its analysis of the data imaged from Server 1, the Organization advised that:

- Server 1 contained 58,170 documents;
- The documents were at least 10 years old;
- Approximately 494 of the documents contained some form of personal information;
- Approximately 200 documents were resumes, employee lists, offer letters, subcontractor agreements, business plans and emails that contained salary and/or bonus information of Synergy's and its clients' personnel (about 200 individuals' names);
- "Sensitive" personal information related to 35 individuals was located, as follows:
 - 1 name with date of birth;
 - 2 names with Social Insurance Number (SIN);
 - 1 name with SIN, date of birth and address;
 - 8 names with SIN and address;
 - 2 names with SIN and address and spouse's names (2);
 - 13 names with SIN, date of birth and salary;
 - 1 name with SIN, date of birth, address, height, weight, marital status and health status (all on an individual's resume);
 - 1 name with SIN, address and old VISA number; and
 - 4 names with old VISA numbers.

According to the Organization, the remainder of the 58,170 documents were business-related and did not contain any personal information.

The Organization also advised that it was able to reacquire Server 2. According to the Organization, its analysis of Server 2 showed that it contained no documents or personal information.

Server 3 was found to be inoperable and the Organization's forensic IT experts were unable to access any information/data on it.

Issue 2: *If the server/s contained personal information, was the information in the custody or under the control of the Organization?*

PIPA applies to all personal information in the custody or under the control of an organization (section 4(1) of the Act). An organization has custody of personal information when it has physical possession. An organization has control of information when it does not have physical custody but has the authority to manage the information (e.g., information held by a contractor on behalf of the organization).

In this case, the personal information on Server 1 originally belonged to Synergy and related to its personnel and its clients' personnel. EY acquired Synergy in 2003, prior to the sale of the servers to the Complainant in 2006. Therefore, Server 1 appears to have been in the custody of the Organization at the time of the sale. As such, the Organization was responsible for the personal information contained on the server.

Issue 3: *If the server/s contained personal information, did the Organization disclose personal information in contravention of PIPA?*

Although not intentional, in selling the servers to the Complainant (in particular, Server 1), the Organization inadvertently caused personal information in its custody to be revealed or exposed (i.e., *disclosed*) to the Complainant.

Generally, PIPA requires individuals' consent to disclose their personal information (section 7 of the Act). There is no indication that the Organization had individuals' consent to disclose their personal information to the Complainant.

PIPA does permit disclosure, without consent, in limited circumstances, as set out in section 20 of the Act. However, there are no provisions, under section 20, which would appear to have permitted disclosure to the Complainant. Therefore, the Organization appears to have been in contravention of PIPA when it inadvertently disclosed the personal information to him.

The Complainant has stated that he avoided viewing more information than was required to provide limited information to this office for the purposes of investigating the matter (i.e., as evidence). There is no reason to believe that the personal information was disclosed to anyone else. As such, the Organization argued that the scope of any disclosure was limited and associated risks low.

Issue 4: *If the server/s contained personal information, did the Organization meet its duty to protect the personal information, under section 34 of PIPA?*

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.

The Act does not require that security arrangements are perfect, only that they are *reasonable*. The types of safeguards that an organization employs should be appropriate for the nature and sensitivity of the information. The Act also explicitly contemplates that an organization's obligations extend to *disposal* of the information. That is to say, an organization's duty does not end when it is no longer using the information or when the information no longer has utility.

According to the Organization, at the time that the servers were sold to the Complainant (approx. August 2006), its practice was to securely wipe all data from servers, using specialized software, prior to sale or disposal. The Organization stated that if the server was sold to the Complainant with EY data on it, this was an isolated incident and an inadvertent contravention of EY policies.

The Organization had policies/practices, in place, at the time of the sale of the servers to the Complainant to ensure data was wiped prior to disposal or sale. However, at least in the case of Server 1, it appears that the policy may not have been followed. This created a situation where the Complainant, the purchaser of Server 1, found himself in possession of the data. No data was found on Server 2 or Server 3 – it may be that wiping was successfully completed on these devices or that they did not have any information on them to begin with. It is an accepted (and expected) practice to ensure electronic devices are purged of personal information prior to sale or disposal. As such, this would be considered a *reasonable* security arrangement. In my view, in failing to ensure that data was purged from Server 1, the Organization was in contravention of section 34 of PIPA.

The Organization advised that, in 2008, it implemented a Media Sanitization Policy.² The policy requires that every individual who manages a media device is responsible for confirming its sanitization. Any hardware leaving a data centre or data room must have an approved service management ticket confirming sanitization. When a server is set for decommission, all hard drives are wiped, removed and destroyed by way of a secure shredding process. The Organization stated that it does not resell servers, hard drives or other media storage devices.

² A copy of EY's Media Sanitation Policy was provided for my review.

The Organization's incident response

The Complainant has complained that the Organization's response to the matter was inadequate. The Complainant points to the initial interactions he had with the Organization when he first reported the matter to them, as well as the Organization's subsequent attempts to investigate and contain the matter.

The Organization suggested that Server 1, and the data therein, have been securely maintained at the Complainant's business site with appropriate physical safeguards. The Organization also argued that there is no evidence of any misuse of the data. The Organization also pointed to the fact that the terms of the Consent Order provide "additional ongoing protection that specifically address the possibility that copies of EY data may exist on the Devices that Ernst & Young did not have an opportunity to inspect."

The Organization is of the view that it has taken "all reasonably possible actions in the circumstances to ensure that any confidential information of Ernst & Young, including personal information of Ernst & Young employees or of clients of Ernst & Young, continues to remain appropriately safeguarded."

Based on the circumstances, I am of the view that the Organization's incident response was reasonable and adequate, with the exception of one recommendation, as below.

Conclusion and recommendations

Although the Organization had policies and practices in place, related to the wiping of devices, it appears that Server 1 was not properly wiped of data. Based on the findings of the Organization, some of the data is personal information. In my view, this constituted both an unauthorized disclosure of personal information to the Complainant as well as failure to ensure that reasonable security arrangements were in place to protect the information.

I am satisfied that the Organization has dealt with the matter in a reasonable manner and made appropriate efforts to contain the information by way of both technical and legal means (e.g., inspecting and wiping the devices, Consent Orders).

I am also satisfied that the policies the Organization presently has in place are reasonable. According to the Organization's policy, it appears that hard drives and other media storage devices must be wiped, degaussed³ then destroyed. Based on the Organization's submission, it no longer sells decommissioned hardware, such as servers. Therefore, risk of a reoccurrence is likely low.

³ A method of destroying data held on magnetic data storage devices, such as hard disc drives (see <http://en.wikipedia.org/wiki/Degaussing>).

Notification

Section 34.1 of PIPA states:

34.1(1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

(2) A notice to the Commissioner under subsection (1) must include the information prescribed by the regulations.

At the time of writing, the Organization has not provided notification to the Commissioner. **I recommend that the Organization notify the Commissioner, as set out in section 34.1 of the Act and section 19 of the Regulation.** The Commissioner will then determine whether the incident requires notification to affected individuals. Failure to report is an offence under section 59(1)(e.1) of PIPA. More information on breach reporting can be found on our website at <http://www.oipc.ab.ca/pages/PIPA/BreachNotification.aspx>.

I have no further recommendations.

Next steps available in the process

If Mr. Morris believes the matter has not been resolved by this investigation:

- A request can be made to the Commissioner to hold an inquiry into the matter pursuant to section 50 of the Act;
- The Commissioner's decision to hold an inquiry is **discretionary**, meaning the Commissioner may or may not decide to hold an inquiry;
- The inquiry is not an assessment of this investigation or my findings. It is a new evaluation of the issues;
- The Commissioner would consider submissions of both parties and then decide questions of fact and law independent of this investigation process;
- The facts from this investigation will be used in the inquiry process. You will be required to provide a submission for the inquiry process to our Adjudication Unit.

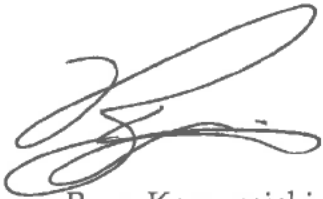
If Mr. Morris wishes to request an inquiry, I must receive a completed "Request for Inquiry" form by **March 25, 2015** (a copy is attached). The form can also be found at our website at <http://www.oipc.ab.ca/pages/PIPA/Inquiries.aspx>.

If I do not receive the form by this date, this file will be closed.

Questions

You may contact the Registrar of Inquiries regarding the inquiry process at 780-422-6860 or toll free within Alberta at 1-888-878-4044. If you have any questions about my review, please call me at the same number.

Sincerely,

A handwritten signature in black ink, appearing to read 'Ryan Komarnicki', with a stylized flourish at the end.

Ryan Komarnicki
Senior Information & Privacy Manager

Enclosures for Complainant:

- *Request for Inquiry Form*
- *Preparing for an Inquiry Brochure*