OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
— for —
British Columbia

INVESTIGATION REPORT F06-01

SALE OF PROVINCIAL GOVERNMENT COMPUTER TAPES CONTAINING PERSONAL INFORMATION

March 31, 2006

Quicklaw Cite: [2006] B.C.I.P.C.D. No. 7
Document URL: www.oipc.bc.ca/investigations/reports/InvestigationReportF06-01.pdf
Office URL: www.oipc.bc.ca

TABLE OF CONTENTS

1.0 INTRODUCTION **2**

2.0 BACKGROUND **2**

3.0 DISCUSSION **4**

3.1 The Investigation Process and Outcome **4**
Retrieving and securing the tapes 4
How did the tapes end up being sold? 7
What personal information is on the tapes? 10

3.2 Reasonable Security Measures for Personal Information **12**
What does “reasonable” mean? 14
Defining and documenting security arrangements 14
Foreseeability of a privacy breach and resulting harm 15
Generally accepted or common practices 16
Medium and format of the record 16
Criminal activity and other intentional wrongdoing 17
Cost of security measures 17
Disposal of personal information 19

3.3 Adequacy of Provincial Government Policies and Procedures **19**
FIPPA Policy and Procedures Manual 20
Core Policy Manual 21
Information Technology Security Policy 22
2002 Direction on Computer Disk Erasures 24
MEIA Procedures 24

3.4 Notification of Affected Individuals 25

3.5 Recommendations 29

4.0 CONCLUSION 31

1.0 INTRODUCTION

[1] Examples abound these days of privacy breaches involving the unauthorized disclosure or acquisition of personal information because of compromised storage, handling or disposal of computer devices or electronic data media. This is so even though security safeguards are available and even though governments and businesses know that they must protect the security, confidentiality and integrity of the personal information they hold. This case illustrates the all too common failure of both public and private sector organizations to ensure that safeguards are identified and diligently implemented throughout organizations.

[2] Simple errors can have great significance, yet simple solutions exist for many of the personal information security challenges that confront organizations in the public and private sectors. This report focuses on identifying solutions that will help public bodies in British Columbia to meet their legal obligations under the *Freedom of Information and Protection of Privacy Act* ("FIPPA") and assist private sector organizations to meet theirs under the *Personal Information Protection Act* ("PIPA").[1]

[3] Before addressing the circumstances of this case, I will set out the relevant factual background.

2.0 BACKGROUND

[4] On Friday, March 3, 2006, a journalist at *The Vancouver Sun* newspaper contacted the Office of the Information and Privacy Commissioner ("OIPC") seeking comment on a story that *The Vancouver Sun* planned to print the next day. The OIPC was told that *The Vancouver Sun* had come into possession of 41 computer data backup tapes containing extensive and sensitive personal information of thousands of British Columbians. These tapes had been sold at a public sale of provincial government assets.

[1] This report addresses public body responsibilities to adopt security measures to protect personal information, found in s. 30 of FIPPA. Section 34 of PIPA uses language very similar to that of s. 30 of FIPPA in requiring private sector organizations in British Columbia to protect personal information by making "reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal or similar risks."

[5] The OIPC was told that the purchaser had turned the tapes over to *The Vancouver* Sun after discovering that they contained personal information. This led to articles in the March 4, 6, 7 and 8, 2006 editions of *The Vancouver Sun*. The gist of the first two articles—which were also picked up by other newspapers—was that, in May 2005, the provincial government had auctioned off computer tapes containing thousands of highly sensitive records (apparently created from 1995 to 2001).

[6] These records contained information about medical conditions (including HIV-positive diagnosis, mental illness and substance-abuse), thousands of individuals' names (with social insurance numbers and dates of birth), details of applications for social assistance, and caseworker entries divulging extremely intimate information about people's lives.

[7] *The Vancouver Sun* did not name any individuals identified in the records, although its articles did describe details of several particular situations without naming the individuals involved. (*The Vancouver Sun* also said it had attempted without success to reach at least one of the individuals for comment.)

[8] The final article in *The Vancouver Sun* broke the further story that, at the May 2005 sale, the purchaser of the 41 tapes had also purchased seven BlackBerry™ devices, which the purchaser said appeared to be filled with emails and addresses, and a login code and password provided to *The Vancouver Sun* were still valid.[2]

[9] On March 3, 2006, I informed officials of the Ministry of Labour and Citizens' Services ("MLCS")—the provincial government ministry responsible for information technology within the provincial government, including disposal of surplus assets—that I would be initiating an investigation of the situation under FIPPA. *The Vancouver Sun* also notified MLCS of the situation on March 3, 2006 and MCLS immediately placed a temporary ban on the sale of memory storage devices and initiated its own investigation.

[10] On March 7, 2006, the Minister of Labour and Citizens' Services, Hon. Mike De Jong, said this in the Legislative Assembly:

> …I am now convinced that there is no ironclad way to ensure that, whatever the scrubbing technology, you can sell computers or information-gathering material safely guaranteeing the security of privacy. The ban that was put in place temporarily will become permanent.[3]

[2] My office later learned that, the purchaser, before going to *The Vancouver Sun*, had deleted all information from the BlackBerry™ devices and sold them. He had, however, given *The Vancouver Sun* some address-book information gleaned from one device and this information was the basis of the March 8, 2006, article.

[3] Legislative Debates of British Columbia, Hansard (Afternoon Sitting, March 7, 2006), p. 2770.

[11] On March 24, 2006, the office of the provincial government's Chief Information Officer ("CIO"), an office within MLCS, reported on its investigation into how the 41 tapes left government custody, came into the hands of a purchaser at public auction and then came into the possession of *The Vancouver Sun*.[4]

[12] This report results from my investigation, under s. 42 of FIPPA, into the disclosure of personal information involved in the sale of the 41 backup tapes and other storage media. This report makes findings, and contains recommendations, but no order is made under s. 58 of FIPPA,

3.0 DISCUSSION

[13] This report is divided into the following parts:

1. Discussion of the OIPC's investigation into unauthorized acquisition or disclosure of sensitive personal information,
2. Discussion of factors to be considered in assessing whether reasonable security arrangements exist to protect personal information,
3. Discussion of the adequacy of the defined and documented government policies and procedures that were in place in respect of this situation,
4. Discussion of notification of affected individuals and
5. Recommendations for action by the provincial government.

3.1 The Investigation Process and Outcome

[14] This part of the report discusses the OIPC's investigation into how the 41 tapes left the custody of the public body responsible for their security.

[15] An investigative team representing the OIPC had unfettered access to relevant materials and individuals during the course of the provincial government's investigation. The OIPC's investigative team consisted of Jim Burrows, Portfolio Officer, and representatives of FDR Forensic Data Recovery Services ("FDR"), a firm of computer experts that the OIPC retained immediately after learning of the incident, to assist with the OIPC's investigation.

Retrieving and securing the tapes

[16] As a first step, the OIPC facilitated the return, on March 6, 2006, of the 41 tapes from *The Vancouver Sun*. The purchaser of the 41 tapes permitted them

[4] CIO Investigation Report 2006-048 (March 24, 2006), "Loss of custody of 41 computer tapes containing personal and sensitive information".

to be returned on the condition that his identity would not be disclosed. The purchaser also swore an affidavit at the OIPC's request, as follows:

1. The purchaser had bought the 41 backup tapes (and some tape readers) from the provincial government at a public sale in the Lower Mainland in or around May 2005 and had delivered all of the tapes to *The Vancouver Sun* around February 2006.
2. The purchaser had not made or kept any copies of the tapes or otherwise copied information on the tapes, including by saving or storing of computer data.
3. The purchaser did not have personal knowledge of anyone else accessing the tapes or any information stored on them before they were delivered to *The Vancouver Sun*.

[17] On March 6, 2006, my office learned that *The Vancouver Sun* had copied personal information that it had used for its articles onto one DVD disc and three CD discs. Representatives of my office communicated with *The Vancouver Sun* and its representatives and ultimately we were satisfied with *The Vancouver Sun*'s proposal for securing those materials and its assurances as to its use of personal information on the tapes.

[18] On March 7, 2006, an employee of FDR and Jim Burrows of the OIPC, who conducted our investigation of this matter, placed the 41 backup tapes in a locked cabinet in the secure server room within the facilities of MLCS's Common Information Technology Services Branch ("CITS"). The tapes became the responsibility of the CIO's Information Security Branch ("ISB").[5]

[19] Under the OIPC's direct oversight, the ISB then began the process of restoring the tapes to fully-wiped hard drives. Once restoration was complete, the restored folders were copied into EnCase logical evidence files, thus providing a forensic copy of the data without disturbing file metadata. The software also allows detailed analysis of the available data. The process of restoration and analysis was still ongoing as of March 24, 2006, when the CIO's report was issued. This is to be expected given the age of the tapes and the volume of the material.

[20] The OIPC investigated the circumstances surrounding how the tapes came into the purchaser's hands. A similar investigation was undertaken by the ISB at the same time. The ISB and other provincial government agencies and staff co-operated fully in sharing information and records. The OIPC's investigator interviewed provincial government employees who had knowledge of the events leading up to the sale of the tapes and of the policies and standard practices of the Ministry of Employment and Investment ("MEIA"), the ministry

[5] The server room requires card access for entry. Both the cabinet lock and the server room door lock log any users accessing them. FDR reviewed these logs on our behalf from time to time.

from which the backup tapes and hard disk drives mentioned below had originated.

[21] During the investigation, my office became aware that a number of computer server hard disk drives had also formed part of the auction lot that contained the 41 tapes. The purchaser of the tapes and hard drives gave assurances to my office that he had not yet examined the drives. My office asked the purchaser to examine one of the hard drives to see if it had been properly wiped as required by government policy. After examining one of the drives, the purchaser notified us that the hard drive had not been wiped and that government data was accessible on the drive.

[22] We then arranged for the purchaser to sell the servers and hard drives back to the province and he agreed to this on March 24, 2006. The servers and hard drives were picked up by FDR in the Vancouver area in a similar manner to the tapes. On March 28, 2006, they were delivered then to the ISB, which, under FDR's supervision, examined the equipment and determined that there was information similar to that present on the 41 tapes.

[23] Included in the items recovered were 17 individual computer hard-disk drives and five other drives still attached to a Compaq server. The purchaser had labelled the drives from which he had been able to recover data. After the drives were photographed and counted, two drives with handwritten labels marked "data recovery" were examined.

[24] These two drives were forensically previewed and copied on March 29, 2006. On the basis of the preliminary analysis of these drives, it was confirmed that although one "data recovery" drive had no intact file structure, there were many thousands of records containing personal information including GAIN ID, name, address, phone numbers and case-worker notes. These records apparently originated in 2000 from what was at the time the Ministry of Social Services and is now MEIA.

[25] Preliminary analysis of the second of these two "data recovery" drives disclosed no reference to any GAIN IDs, although this drive did appear to have data on it. No other searches were performed on this drive.

[26] I directed on March 29, 2006 that FDR should not, at this time, conduct any further analysis of the remaining drives. ISB employees indicated that they would continue their analytical efforts.

[27] I took this step because of concern that this report not be delayed. This means that not all of the newly-retrieved drives have been analyzed exhaustively. The recent retrieval of these other pieces of equipment also means that the events leading up to their sale have not been investigated definitively. However, in light of the purchaser's assurances as to his custody of the

equipment, the fact that this material formed part of the same sale lot, and the fact that they contained similar information, I will, for the purposes of this report, treat the sale of these drives, and the resulting unauthorized disclosure of personal information, on the same basis as the 41 tapes that were sold to the same purchaser as part of the same sale lot.

How did the tapes end up being sold?

[28] Our review of records provided to us, and information obtained from interviews with knowledgeable MEIA[6] staff, led me to draw the following conclusions.

[29] Before February of 2005, it was decided that MEIA's office at 590 West 8th Avenue in Vancouver ("Vancouver office") would close.[7] This office had a server room and adjoining area that were used by MEIA's Information Management Branch. Staff began to make preparations early in 2005 even though the final move was not slated to occur until July of 2005. Preparations included the identification of 507 computer backup tapes for computer servers used at that office.[8] Up until April 2004, these tapes had been used on a regular basis, either weekly or monthly, to back up the computers and servers and to permit disaster recovery if needed.

[30] In April of 2004, CITS took over the process of backing up computer servers over the government network rather than using backup tapes on a location by location basis. Because the 507 backup tapes for the Vancouver office had become redundant, in September of 2004, MEIA Information Management Branch staff sought authorization to destroy them. Consent was given on February 11, 2005 through a Records Destruction Authorization form signed by MEIA's Records Officer.

[31] The backup tapes were stored in a cabinet in an area adjoining the server room, referred to as the staging area. Entry to the area was through a locked door, which required card access. At some time during the early months of 2005, MEIA staff boxed the 507 tapes and left them in front of the cabinet. No inventory of the tapes was conducted and the boxes were not labelled as to their contents. MEIA staff estimated that roughly 40 to 50 tapes could have been stored in a box of the size used. This estimate suggests that there would have been at least ten or eleven boxes of tapes on site.

---

[6] At the time of the events in question here, MEIA was known as the Ministry of Human Resources. It is referred to throughout this report as MEIA.

[7] Government staff had noted that a photograph of the tapes published in the March 4, 2006 edition of *The Vancouver Sun* showed one of the tapes was labelled "VAN590W8TH". Examination of the tapes after their retrieval confirmed that some of the other tapes were also labelled this way, while different label information was present on other tapes and some tapes had no labels at all.

[8] This number is approximate, since MEIA staff confirmed that an exact count of the tapes was not done and information tapes were never inventoried because there were so many.

[32] MEIA staff confirmed that they intended to have all 507 backup tapes destroyed. They said this would be done under contract with Recall Secure Destruction Services ("Recall"), the provincial government's contractor for the disposal of confidential records. A Recall invoice dated March 7, 2005 shows that non-recyclable material was picked up on February 15, 2005. However, it is unlikely that the 507 tapes were picked up at this time, as the quantity of material which was shown on the invoice was not large enough to be a description of that many tapes. Further, the Team Leader of MEIA's Information Management Branch remembered that he placed the boxes of tapes beside the shredding bins, for pickup by Recall close to the time of the Vancouver office's move on July 8, 2005.

[33] Invoices from Recall corroborate this. On June 28, 2005 and July 7, 2005, Recall removed a significant amount of material designated "destock" from the Vancouver office. MEIA staff confirmed with Recall, for the purposes of this investigation, that the term "destock" is used to identify material such as tapes, microfiches and diskettes. Based on the information provided by MEIA staff and review of the available records, it is likely that Recall picked up most of the 507 tapes at the end of June and beginning of July for destruction.

[34] Interviews with a number of staff who were present during the Vancouver office's moves confirm that there was a considerable amount of disruption and that many boxes and types of computer equipment were piled throughout the staging area.

[35] After computer equipment was removed from the server room and prepared for disposal, it was placed together in groups until arrangements for pickup by MLCS's Asset Inventory Recovery ("AIR") branch. One such group, consisting of servers, monitors, uninterrupted power supply equipment and two tape drives, was assembled before March 2, 2005. A March 2005 Asset Transfer and Disposal Report confirms that AIR was called to pick up this material and that it did so on March 14 or 15, 2005. The report does not list any tapes among the materials turned over to AIR, but MEIA was not able to identify any other AIR pickups before June of 2005. Since the 41 backup tapes were sold in May of 2005, it may be that the March 2005 AIR pickup included the tapes.

[36] It is not possible to arrive at any definitive answer as to how the 41 backup tapes came to be part of a lot of computer equipment sold by AIR in May of 2005. MEIA, AIR and other provincial government staff were forthright and open in providing information for the purposes of this investigation, but the absence of proper documentation makes it impossible to know with certainty what happened. Given the timing of the sale of the 41 tapes in May of 2005, and given the fact that there was considerable disruption and disarray in the server room and staging area because of the Vancouver office's move, a plausible explanation is that a box containing the 41 tapes was inadvertently placed on the pile of

computer equipment to be picked up by AIR in March of 2005 and was sold as part of a lot of materials in May of 2005. In my view, the best available evidence is that MEIA staff accidentally turned the tapes over to AIR.

[37] It is worth emphasizing here that the failure of the MEIA and AIR to properly document their actions in relation to the tapes makes it impossible to say with any certainty what happened. There was no proper inventory by MEIA or other provincial government staff of the 507 tapes designated for destruction. There was no proper record of the process for transferring possession of the tapes and ensuring their destruction. No record exists of which we are aware that identifies each tape delivered to and destroyed by Recall in the summer of 2005. There was no proper inventory of the material AIR acquired from MEIA, with a view to identifying materials that should be destroyed and ensuring that was done. Later in this report, I make recommendations aimed at ensuring these deficiencies are corrected.

[38] There is no need to repeat here all of the details set out in the CIO's report. Given the similarities between the factual conclusions that our investigation yielded and those expressed in the CIO's report, it suffices to note that the CIO's investigation found the following:

1. Unwiped computer backup tapes containing extensive sensitive personal information connected to programs or services of MEIA and the Ministry of Children and Family Development ("MCFD") were sold in May 2005 by AIR.

2. AIR's original transaction records for the sale lot believed to have contained the 41 tapes and the BlackBerry™ devices have been located and have been sealed to maintain the confidentiality of the purchaser.

3. The tape readers purchased in the same lot as the 41 tapes originated with the federal government, for which AIR also conducts asset disposal.

4. Twenty-one of the 41 tapes were physically marked as originating from a MEIA office in Vancouver that closed in July 2005. Other tapes were not labelled. None of the tapes was labelled for or assigned a resident data content or sensitivity level. Nor were any of them encrypted or inventoried.

5. MEIA had policies in place that expressly prohibited the sale of computer data tapes.[9]

[9] The written MEIA procedures brought to our attention during our investigation relate to destruction of records in a very general way and are in my view inadequate for dealing with electronic storage media and devices. In light of my recommendation that a government-wide policy to deal with electronic information be created, there is no point analyzing MEIA policies in any detail.

6. MEIA staff who were responsible for handling of computer equipment and data media at the Vancouver office were aware of requirements and procedures for the destruction of tape media.

7. MEIA staff apparently believed that "wiping" applied to hard drives only and did not apply to data storage media.

8. Around the time of the impending MEIA office move, there was loose unattended material, boxes and supplies throughout the building.

9. Similar-looking boxes containing tapes for destruction and computer equipment designated for asset disposal were stored in a secure server room onsite.

10. AIR staff practice was to destroy data tapes and other removable media originating from provincial ministries.

11. The listing of assets sent from the MEIA office for disposal or destruction was incomplete.

12. AIR had no inspection or quality assurance process in place to detect the tapes before they were put into a lot for public sale.

What personal information is on the tapes?

[39] At the same time the ISB was copying and securing the 41 tapes for analysis, my office and provincial government representatives agreed on an approach for analyzing the tapes' contents. It was agreed that the tapes would be analyzed by FDR using the following information-classification template:

Personal Information
- Name (surname and first name)
- Date of birth or age
- Child and Youth information

Unique Identifiers
- Social Insurance Number
- Driver's licence number
- Medical Services Plan number
- Other identifiers (GAIN[10], Immigration, etc.)

[10] GAIN refers to social assistance benefits.

Specific Descriptions or Attributes

- Medical
- Employment
- Financial
- Immigration
- Solicitor / Client
- Other

[40] On March 14, 2006, FDR provided its preliminary analysis of the tapes' contents.[11] I do not propose to describe in detail what FDR found. Some of the readable tapes contained no personal information.[12] Seventeen of the tapes could not be read using common Windows operating systems.[13] Attempts have been since made to read these tapes using various other computer programs and additional personal information has been found.

[41] The remaining five tapes did, however, contain substantial amounts of personal information. The tapes contained backups of two sets of information. Tapes 1, 19 and 41 were backups, likely monthly, of a server file system. Tapes 31 and 39 were backups, also likely monthly, of personal folders. Tapes 1, 19 and 41 contained primarily the same information, the differences being incremental changes to the data between backups. Similarly, tapes 31 and 39 appeared to be backups of the same set of information.

[42] While the number of tapes containing information that was readily accessible on examination was relatively small, a large amount of personal information was stored on the five tapes and, as originally reported by *The Vancouver Sun*, the personal information was highly sensitive. I see no need to exhaustively catalogue here all of the kinds of personal information found on these tapes. It suffices to say that, in addition to containing identifying information such as names, dates of birth, social insurance numbers and personal health numbers, the tapes contained information relating to financial status, social and behavioural disorders, criminal charges, medical information, sexual abuse and substance abuse. These categories of personal information are among the most sensitive imaginable, making the unauthorized disclosure of personal information that occurred here all the more significant, and regrettable.

[43] The next step is to consider what s. 30 of FIPPA entails for personal information security measures on the part of public bodies in British Columbia.

---

[11] As of that date, attempts were still underway to restore seventeen of the tapes. Initial attempts to restore these tapes resulted in a "foreign tape" report. FDR suggested that this may have been due to use of different backup software than the Windows NT4 software used to back up the tapes that were readable.

[12] FDR reported that it found no personal information on tapes numbered 3, 4, 5, 7, 8, 9, 12, 13, 16, 18, 20, 22, 23, 24, 25, 28, 34, 38 and 40 at that date.

[13] Tapes 2, 6, 10, 11, 14, 15, 17, 21, 26, 27, 29, 30, 32, 33, 35, 36 and 37.

3.2 Reasonable Security Measures for Personal Information

[44] This part of the report discusses material aspects of public bodies' duty under s. 30 of FIPPA[14] to implement reasonable security measures to protect personal information.

[45] Part 3 of FIPPA applies to "personal information", which it defines as follows:

> "**personal information**" means recorded information about an identifiable individual other than contact information.[15]

[46] Section 30 is the key provision in Part 3 for ensuring the security of personal information held by public bodies. It reads as follows:

> **Protection of personal information**
>
> 30. A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

[47] As does this investigation, my office's 2004 USA Patriot Act report[16] presented an opportunity to consider the meaning of s. 30. The relevant portions of that discussion merit quotation at some length:

> The British Columbia government has provided dictionary definitions of 'reasonable' that it says indicate "reasonable security arrangements" are arrangements that are sensible and proportionate to the type of personal information involved. We agree that reasonable security arrangements are not infallible arrangements, not the least because such arrangements would be impossible. We agree, too, that the nature of the personal information involved and the seriousness of the consequences of its unauthorized disclosure are factors to be taken into account in assessing the reasonableness of security arrangements. The highly contextual approach to informational privacy that is evident in Charter [of Rights and Freedoms] case law may be instructive in this regard, as may the following example from the OIPC's guidelines for public bodies to refer to in designing, and auditing the performance of, automated systems that contain, process, transmit or otherwise deal with personal information:

---

[14] Section 34 of PIPA, as noted above.

[15] FIPPA, Schedule 1, which also defines "contact information" as "information to enable an individual at a place of business to be contacted and includes the name, position name or title, business telephone number, business address, business email or business fax number of the individual".

[16] *Privacy and the USA Patriot Act—Implications for British Columbia Outsourcing*. <www.oipc.bc.ca/sector_public/usa_patriot_act/pdfs/report/privacy-final.pdf>

> A variety of circumstances—including the nature of the personal information involved and the uses for that information—will determine which measures are necessary in each case to protect personal privacy and ensure the security of personal information. For example, a self-governing body need not, in creating a list of members' names and addresses, take the same measures for the privacy and security of that limited personal information as a hospital would have to take respecting patients' personal medical information.[17]

We do not, however, agree with the BC government's submission that orders of the Information and Privacy Commissioner about whether a public body has made every 'reasonable' effort to assist an applicant for access to information, as section 6 of FOIPPA requires, are helpful in the context of section 30. We say this because the consequences of the conduct involved must be considered in measuring the degree of vigilance that is reasonably required. Most problem situations under section 6 of FOIPPA can be corrected. In many instances, lax effort in assisting an applicant means a response to an access request is provided later rather than sooner or the applicant gets a series of corrected responses instead of a thorough response the first time around.

Unauthorized disclosure puts private information where it should not be and lax security arrangements create risk that this generally more serious consequence will be realized. Attempting to remedy the unauthorized disclosure of personal information is another matter, especially if the information is disclosed to those who are consciously seeking access for their own purposes, without regard to the privacy protections in FOIPPA.

…

It must not be forgotten, as well, that although particularly rigorous security arrangements will be reasonably required for information that is closer to the biographical core of the individual (the unauthorized disclosure of which will have more serious consequences), the requirement for security arrangements is not removed when more attenuated privacy interests are involved. Security arrangements are required to protect against any unauthorized disclosure of personal information. The fact that there is not likely to be any interest in particular information or that it would not occur to anyone to look or ask for it can never be a substitute for security arrangements to protect that information.[18]

[48] This investigation offers an opportunity to expand on the above discussion by outlining some factors for the application of the reasonableness standard in and by discussing the question of notification of affected individuals of privacy

[17] *Guidelines for Data Services Contracts* (OIPC Guideline 01-02) http://www.oipc.bc.ca/advice/Guidelines-Data_services.pdf.
[18] USA Patriot Act Report, pp. 110-111.

breaches involving their personal information. To do this, I have drawn on standards, investigation reports, public reports and other resources.[19]

What does "reasonable" mean?

[49] By imposing a reasonableness standard in s. 30, the Legislature intended the adequacy of personal information security to be measured on an objective basis, not according to subjective preferences or opinions. Reasonableness is not measured by doing one's personal best. The reasonableness of security measures and their implementation is measured by whether they are objectively diligent and prudent in all of the circumstances. To acknowledge the obvious, "reasonable" does not mean perfect. Depending on the situation, however, what is "reasonable" may signify a very high level of rigour.

[50] The reasonableness standard in s. 30 is also not technically or operationally prescriptive. It does not specify particular technologies or procedures that must be used to protect personal information. The reasonableness standard recognizes that, because situations vary, the measures needed to protect personal information vary. It also accommodates technological changes and the challenges and solutions that they bring to bear on, and offer for, personal information security.

Defining and documenting security arrangements

[51] FIPPA does not expressly require the documentation of security measures, but defining and documenting security arrangements for personal information—and implementing training and oversight to ensure that those arrangements are understood and applied—is diligent and prudent practice for the purpose of measuring the reasonableness of security arrangements under s. 30 of FIPPA.

[19] These include Canada's *Model Code for the Protection of Personal Information* CAN/CSA-Q830-96 (1995) (developed by the Canadian Standards Association and forming Schedule 1 to the Canada's federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act*); the International Information Security Standard ISO/IEC 17799: 2005; *APEC Privacy Framework* (2004); Office of the Victorian Privacy Commissioner, Report 01.06, *Jenny's Case* (February 2006); US Federal Trade Commission, *Prepared Statement to the U.S. Senate Committee on Commerce, Science and Transportation on Data Breaches and Identity Theft* (June 6, 2005); California Office of Privacy Protection, *Recommended Practices on Notification of Security Breach Involving Personal Information* (October 10, 2003); Ontario Information and Privacy Commissioner, *Identity Theft Revisited: Security is Not Enough* (September 2005); Ontario Information and Privacy Commissioner, Order HO-001 (October 2005); Ontario Information and Privacy Commissioner, Privacy Complaint No. PC-020036-1 (July 8, 2003); Alberta Information and Privacy Commissioner, Investigation Report H2005-IR-001.

Sensitivity of the personal information

[52] The sensitivity of the personal information at stake is a commonly cited,[20] and important, consideration. For example, a computer disk or paper file containing the names of a local government's employees who are scheduled to attend a conference or take upcoming vacation does not call for the same protective measures as a disk containing the medical files of those employees.

[53] Sensitivity is a function of the nature of the information, but other factors will also affect sensitivity. For example, the sensitivity of medical treatment information for someone who died 70 years ago is less than for someone who died more recently or is living.

Foreseeability of a privacy breach and resulting harm

[54] Information security measures are properly established through a methodical assessment of risk that assesses both the foreseeability of a privacy breach (intentional or accidental) occurring in the context of current threats to or weaknesses in existing information-security measures and the severity and extent of the foreseeable harm that could result from a privacy breach. This assessment is then used to identify and implement a hierarchy of security measures according to the degree of risk involved.

[55] A security breach involving sensitive personal information will, unless it is quickly and completely rectified, almost always give rise to foreseeable risk of significant harm. This could be pecuniary harm (for example, loss of business or employment opportunities) and non-pecuniary harm (for example, hurt, humiliation, damage to reputation and damage to relationships with family, friends, colleagues or even the public).

[56] Sometimes a security breach that involves personal information that is neither sensitive nor particularly private—for example, a credit card number and expiry date in conjunction with the cardholder's name—can create a foreseeable risk of serious harm in the nature of financial fraud or identity theft.

---

[20] See, for example, Clause 4.7.2 of the 1995 *Model Code for the Protection of Personal Information* (Canadian Standards Association, CAN/CSA-Q830-96). The CSA Code forms Schedule 1 to the federal private sector privacy law, the *Personal Information Protection and Electronic Documents Act*. Also see, for example, the *APEC Privacy Framework*, Principle 22 <www.apec.org/apec/apec_groups/som_special_task_groups/electronic_commerce.html)>.
The provincial government's *Policy and Procedures Manual* for FIPPA, which applies to provincial government ministries, also identifies the sensitivity of personal information as a factor. <http://www.mser.gov.bc.ca/privacyaccess/manual/sections/sec30_39/sec30.htm>.

Generally-accepted or common practices

[57] Generally-accepted information management practices or technical standards in the public or private sectors may be relevant under s. 30. An information management practice may be common, but not be generally accepted as an adequate or good practice. Nor is it likely to be sufficient to follow a common practice that is not a demonstrably reasonable practice. The fact that a generally-accepted and proven practice has been followed may be strong evidence of prudence and diligence in protecting personal information, but it is not determinative. If such a practice or technical standard clearly does not accord with objective prudence and diligence, then s. 30 will not be met. In other words, generally accepted practices and technical standards must be complemented by elementary caution and common sense.

Medium and format of the record

[58] When personal information is recorded in paper format—for example, in a document located in a working file—loss of the document raises different risks than when personal information is recorded in electronic form and transmitted by email or posted on the internet. Having said this, personal information in paper format can readily be scanned into electronic form or photocopied and widely distributed by email, fax or other means. The ease of paper-to-electronic transformation suggests that the practical obscurity that is often considered to be a feature of paper records is less meaningful than many observers have contended.

[59] For records in electronic form, consideration must be given to whether personal information is encrypted[21] or is recorded in a format that can be read using equipment and knowledge that are readily available to someone with an average knowledge of computers and information technology. Depending on the circumstances, it may not be reasonable to hold or move sensitive personal information in a readily-available electronic format that is not protected by encryption.

[60] In the United States, a number of states have laws that require organizations to notify individuals of security breaches affecting their personal information, but these requirements often do not apply to encrypted personal information.[22] This acknowledges the effectiveness of encryption as a means of addressing the risks associated with security breaches involving personal information. If personal information is properly encrypted, its security will be

21 One can define "encryption" to mean the use of any of a number of methods to obscure information so as to prevent anyone except the intended reader or recipient from understanding the encrypted information. There are many types of encryption and encryption is now commonly considered to be the basis of network security. Passwords or other controls such as biometrics that are applied to control access to information that is recorded in an electronic device are not methods of encryption.

22 See, for example, California Civil Code, §§1798.82 and 1798.29.

reasonably assured, even if the device or medium containing the information is improperly disposed of or acquired.

[61] The fact that personal information is recorded in an electronic format that, due to specialization or obsolescence, cannot be understood without uncommon equipment or knowledge does not qualify as a security measure for s. 30 purposes. The happenstance of obsolescence or specialization is not a substitute for assessing risk and taking positive security measures to protect personal information.

Criminal activity and other intentional wrongdoing

[62] Ontario's Information and Privacy Commissioner appears to have suggested that criminal activity is an exceptional circumstance that is not encompassed within the standard of reasonable security measures.[23] I agree that the taking of reasonable security measures cannot be a guarantee against criminal activity. In my view, however, the risk of a privacy breach due to criminal activity or other intentional wrongdoing is contemplated in assessing reasonable security arrangements for the purposes of s. 30 of FIPPA. Security measures must be reasonably responsive to such risks, as is the case in other areas. For example, the real risk that criminals will rob a bank, or that bank employees might defraud the bank, does not cause a bank to leave its money unsecured.

[63] There is no presumption of risk to personal information by reason of criminal activity or other intentional wrongdoing or any presumption the other way. For security measures to be reliable, individuals responsible for them need to discharge their functions honestly, diligently and capably. These are qualities that can be established and monitored, reasonably, by systems for information management oversight, training and quality assurance.

Cost of security measures

[64] The question arises of the relationship between the cost and reasonableness of security measures to protect personal information. In discussing s. 4(2) of FIPPA, I considered the relationship between the cost of severing information protected from access under FIPPA and the s. 4(2) duty of a public body to reasonably sever protected information and disclose the rest:

> …[o]ne is not required to altogether ignore the burden of severing a record when considering whether protected information can "reasonably" be severed. There will be cases where the cost of severing is very great while the part of the record that remains after severing, reasonably viewed, is perhaps not entirely incoherent and meaningless, but nonetheless is without informational value.[24]

[23] Privacy Complaint No. PC-020036-1 (July 18, 2003), [2003] O.I.P.C. No. 176, para. 38.
[24] Order 03-16, [2003] B.C.I.P.C..D. No. 16, para. 59.

[65] In the next paragraph of that decision, I quoted my predecessor when he said this:

> …While financial, practical, and technical considerations may be relevant to deciding whether excepted information can reasonably be severed from a particular record, I must be careful not to interpret section 4(2) of the Act in a manner which would undermine the Act's stated purpose of promoting more open and accountable public bodies. In the particular circumstances of this application, and having regard to both the affidavit evidence and submissions before me, I am not persuaded that, had it been necessary for the Board to do so, any third-party personal information could not, for financial, practical, or technical reasons, be "reasonably severed from" the tapes. I might conclude otherwise in some extraordinary cases but this is not such a case.[25]

[66] In our *USA Patriot Act* report, we rejected the proposition that cost savings to the public purse that were said to be gained from the outsourcing of public services to private sector service providers were relevant in deciding whether the government had met its s. 30 obligations to make reasonable security arrangements to protect personal information:

> …we see danger in allowing the question of whether, or the degree to which, outsourcing a public body function is a cost saving for the public body to be a driving factor in determining the adequacy of security measures for the personal information involved. One aspect of providing less costly service could obviously be to provide less security for personal information. Lax security protections could be reasonable because they cost less. This result would be a formula for rapid, unprincipled, erosion of security protection under section 30—essentially a race to the bottom.
>
> …
>
> Personal privacy is a fundamental value in a democratic society. Government efficiency is important too, of course, but it is a tool in the service of other objectives. Efficiency will describe the quicker and most opportunistic way to proceed and sheer efficiency may occasionally serve fundamental values well. But often it will not. It may be difficult or impossible to restore privacy when it is compromised by efficiency—including the sense of privacy in our day-to-day activities that we so cherish yet also tend to take for granted. Efficiency interests, on the other hand, can be accommodated by various means and must not be confused with or trump fundamental values that governments exist to serve and protect.[26]

[67] If a particular security measure offers a minute security benefit at very high cost or impracticable complexity, then it may not be a reasonable

[25] Order No. 205-1997, [1997] B.C.I.P.C.D. No. 67, p. 7.
[26] USA Patriot Act report, p. 115.

component of the security arrangements required by s. 30. On the other hand, a public body cannot dilute the reasonableness standard in s. 30 by insisting on using an inappropriately insecure medium or format for holding or moving sensitive personal information—such as unencrypted data in a widely and readily available electronic format—then decline for cost reasons to adopt other security measures necessary to protect the personal information involved.

Disposal of personal information

[68] Every public body's responsibility for the security of personal information contained in records in its custody or under its control persists throughout the information's life cycle and includes arrangements for secure and permanent disposal by means that are appropriate to the data storage medium and format involved.

3.3 Adequacy of Provincial Government Policies and Procedures

[69] This part of the report addresses the adequacy of the defined and documented government policies and procedures that were in place for the handling and disposal of the 41 tapes, whether those policies and procedures constituted reasonable security arrangements under s. 30 and whether, in any event, changes and improvements are called for.

[70] A first question is whether personal information stored on the 41 tapes in issue here was exposed to unauthorized access, collection, use, disclosure or disposal. In some cases this may be a difficult question to answer. In this case, however, it is clear that personal information was exposed to unauthorized access, collection, use, disclosure or disposal.

[71] The CIO's report suggests that the most likely explanation for the movement of the un-erased backup tapes, hard disk drives and BlackBerry™ devices from government custody to public sale of government assets was a series of procedural and human errors that went undetected and were compounded because of a lack of system checks and balances. Because of this, a wide range of highly sensitive personal information was placed at risk of unauthorized access collection, use, disclosure and disposal. I consider that, at the very least, the disposal of the personal information was not authorized and its disclosure was not authorized.

[72] A second question is whether, before this breach, the responsible public bodies made reasonable security arrangements for protecting personal information stored on the 41 tapes against such risks. The answer in this case is that, whatever written policies or procedures were in place, reasonable security measures were clearly not taken. The many human errors and system gaps[27]

[27] These were particularly in evidence at the Vancouver office of MEIA, where the tapes appear to have originated.

that our investigation detected, and that the CIO's report confirms, fell far short of objectively reasonable security arrangements, bearing in mind the very sensitive and extensive personal information at stake, the relatively simple steps that could have been taken to ensure the safe and proper disposal of the personal information and the predictability of risk of disorder at the time of an office move.

[73] Against this backdrop of information security failures, I will now examine the adequacy of relevant written MEIA and AIR policies and procedures existing at the time of the unauthorized disclosure and of provincial government policies respecting s. 30 of FIPPA. Recognizing that the CIO's report makes recommendations for improvements in relation to information security measures, I will also assess those recommendations and make further recommendations.

FIPPA Policy & Procedures Manual

[74] Provincial government ministries are individually responsible for their compliance with s. 30 of FIPPA.[28] However, the provincial government has a central agency that is responsible for policy respecting information and privacy matters.

[75] IPPB's web page says this about its role:

> The Information Policy and Privacy Branch (IPPB) is part of Strategic Planning and Policy within the Office of the Government Chief Information Officer. IPPB is responsible for the *Freedom of Information and Protection of Privacy Act*, the *Electronic Transactions Act*, the *Document Disposal Act*, the *Personal Information Protection Act* (Private Sector Privacy) and all policy, standards and directives that flow from these pieces of legislation. In addition, IPPB oversees policy related to Information Technology, Information Management, the Corporate Authentication Project and other strategic corporate initiatives of the CIO's office.[29]

[76] IPPB is responsible for the FIPPA *Policy and Procedures Manual*,[30] published by MLCS. It applies to all provincial government ministries. It offers the provincial government's interpretation of FIPPA and policies relating to FIPPA. It does not override FIPPA, of course. The FIPPA *Policy and Procedures Manual* contains the following policy statements regarding s. 30:[31]

1. Public bodies must:

   - ensure their employees are trained to follow proper security procedures;

[28] FIPPA recognizes each ministry as a separate public body and the "head" of each ministry for FIPPA purposes has certain responsibilities under that legislation.
[29] http://www.mser.gov.bc.ca/privacyaccess/
[30] http://www.mser.gov.bc.ca/privacyaccess/manual/toc.htm
[31] http://www.mser.gov.bc.ca/privacyaccess/manual/sections/sec30_39/sec30.htm

- monitor their employees' compliance with security standards;
- ensure physical and procedural security precautions are established and maintained at appropriate levels; and,
- comply with the CORE security access matrix for recorded information.

2. Public bodies shall analyze the types and level of sensitivity of the personal information in their custody and control. Public bodies shall follow the directions on security of information, provided in CORE[32] Chapter 12 and take the necessary steps, over time and within available resources, to implement those physical and procedural safeguards.

[77] Regarding procedures for destruction of personal information, the manual says, at p. 3 of the discussion of s. 30, that "authorized disposal of information" may occur through

> …physical destruction of the record containing the personal information in such a way that it cannot be retrieved or reconstructed (e.g. paper records should be shredded, burned or pulped; magnetic media should be erased or physically destroyed).

[78] At p. 6, the manual gives an example of "unauthorized disposal". It says that destroying sensitive medical records by throwing them into a garbage can, instead of incinerating or shredding them, would be unauthorized disposal.

[79] As regards the specific language of s. 30, the manual says that, for provincial government ministries, which are subject to the Core Policy Manual, "reasonable security arrangements" are "those as provided for" in the Core Policy Manual (p. 4).

Core Policy Manual

[80] The Core Policy and Procedures Manual is the provincial government's central policy instrument on a variety of matters. It deals with information management in section 12.3.2. At p. 10, the manual stipulates that the Corporate Records Management Branch of MLCS[33] does these things:

- establishes standards for secure and confidential destruction of records;
- may monitor the records destruction operations of ministries and other agencies;
- advises ministry records officers on deficiencies of security, economy, efficiency measures; and

[32] The provincial government's *Core Policy and Procedures Manual*, issued by the Office of the Comptroller General.
http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm
[33] Now the Corporate Information Management Branch of MLCS.

- identifies inadequate procedures or processes.

[81] Also at p. 10, the Core Policy and Procedures Manual says this:

> Records destruction operations must maintain the security of information and protect the privacy of individuals whose personal information is contained in records.

[82] The manual provides, at p. 18, that ministries

> …are responsible for ensuring that the electronic storage, retention and disposition of data are consistent with government records management policies, in accordance with *Document Disposal Act* and the *Freedom of Information and Protection of Privacy Act*.

[83] It adds that Ministry Records Officers in each ministry "authorize ministry destructions and document the types and volumes of records being destroyed" (p. 10).

[84] As noted in the CIO's report, Chapter 15 of the Core Policy and Procedures Manual provides as follows:

> Each ministry must protect information holdings in all physical, electronic and digital formats commensurate with its value and sensitivity at all stages in the life cycle of the activity to preserve the confidentiality, integrity, availability, intended use and value of all records. Security categories approved by Risk Management Branch must be used.

[85] Chapter 15 also requires ministries to identify and categorize "information and other assets based on the degree of injury (low, medium, high) that could reasonably be expected to result from compromise due to their availability or integrity, with reference to the provisions of the *Freedom of Information and Protection of Privacy Act* or other legislation."

Information Technology Security Policy

[86] In October 2004, the Ministry of Management Services, which at the time was the ministry in which CITS resided, issued the *Information Technology Security Policy* (release 2.2) ("ITSP").[34] The introduction says this about the purposes of the ITSP—which include preserving privacy—and about accountability for compliance with its requirements (p. 1):

> The purpose of the Information Technology Security Policy (ITSP) is to support government organizations in preserving the confidentiality, integrity,

[34] http://www.cio.gov.bc.ca/prgs/ITSP.pdf.

> privacy[35] and availability of IT assets. The ITSP supports the government's core policies and forms a part of the series of reference documents for the Core Policy and Procedures Manual (CPPM) 15 Security, and is applicable to all ministries (see CPPM Governance section 1.2.4 Application). Key roles and responsibilities for ITSP are described in CPPM section 15.2 General.
>
> The ITSP is to be used by all managers, employees, contractors, consultants and other individuals who are collectively responsible for IT systems within the ministry. All other employees are encouraged to become familiar with the ITSP and its provisions.

[87] The ITSP says that ministries must ensure the media are "protected from damage, alteration, theft, loss or unauthorized access" (p. 12). It goes on to say this (p. 12):

> Ministries are accountable for developing and implementing procedures for control, use, and protection of all removable media;
>
> …
>
> Data destruction methods for non-erasable media must be in accordance with government legislation, policies and standards. Erasable media must not be released for reuse, destruction, or resale until it has been sanitized using an approved government erasure procedure.[36]
>
> Ministries must be able to implement proper data destruction methods for confidential or highly-sensitive material, rather than relying on third parties. Some ministry security provisions may require that the media be removed and retained by the ministry, rather than destroying it. In this case, the ministry will exercise the option to replace the media with a new, suitable media of equal or greater capacity.

[88] The ITSP also says, at p. 12, that the "scope of the sanitizing policy for IT asset disposal and reuse includes…asset disposal sales to the public".

[89] As for ensuring that provincial government employees know their responsibilities, the ITSP says this (at p. 15):

> Ministries are responsible for ensuring that all personnel receive security education and training for the safeguarding of IT assets in conjunction with employee safety and security programs.

---

[35] The ITSP refers in several places to FIPPA, *e.g.*, it is listed in Appendix A to the ITSP as a key reference.

[36] At this point, the web version of the ITSP links the reader to a CITS web page entitled "Disk Erasure Procedures". This page identifies three programs approved for erasure of hard disk drives. The page says nothing about erasure of other media, including the backup tapes in question here or BlackBerry™ devices. http://www.cits.gov.bc.ca/serv/disk.htm

2002 Direction on Computer Disk Erasures

[90] In a May 15, 2002 memorandum to all deputy ministers, the then CIO addressed the issue of secure erasure of computer disks before disposal or re-use. In the memorandum, the CIO requested the "cooperation" of deputy ministers in ensuring that "government computers are erased of all information prior to asset disposal" or otherwise being disposed of. The memorandum said that disk erasure policies had been updated and cited them. The memorandum went on to say this:

> These revisions define a minimum baseline for ensuring that computer disks are erased prior to disposal to prevent disclosure or recovery of personal and government information. This minimum baseline fulfils statutory obligations under Section 30 of the *Freedom of Information and Protection of Privacy Act* (FOIPP Act) to protect personal information.

[91] The memorandum only addressed computer disk erasure. It did not mention secure erasure or destruction of backup tapes or other storage media.

MEIA Procedures

[92] As noted above, the CIO's report on this incident says

> MEIA had procedures in place that expressly prohibited the sale of computer data tapes. Staff were aware of and trained in these procedures as is demonstrated by the documented destruction of tapes throughout 2005.

[93] The CIO's report refers to specific portions of relevant government-wide policy, but does not quote from or otherwise cite any such MEIA policy. The written procedures brought to our attention during our investigation are in my judgement inadequate for dealing with destruction of electronic storage of personal information, but in light of the following discussion—and my comments below in the section on recommendations—I see little to be gained in detailing the reasons for this conclusion.

[94] There can be little debate about the inadequacy of existing provincial government policies and procedures respecting the secure destruction of personal information found in the wide variety of storage media and devices now in use within the provincial government. As the CIO's report indicates, many provincial government ministries have not created procedures for the destruction of removable storage media, despite their obligation to do so according to central government policy.

[95] The CIO's recommendations, I note, suggest that the government recognizes the need for centralized, consistently and rigorously implemented policy and procedures respecting the secure erasure and destruction of personal information. From my perspective, the provincial government has little time to lose in moving forward aggressively in this area.

3.4 Notification of Affected Individuals

[96] Several observers have suggested that, in this case, the government should give notice to each individual involved that their personal information has been disclosed. This section of the report considers whether the relevant public body or public bodies should give notice, individually or collectively, to the thousands of individuals whose personal information is involved.[37]

[97] Many of the United States have in recent years enacted laws requiring organizations responsible for privacy breaches to notify affected individuals. Since 2003, for example, California law has in certain circumstances required organizations to notify individuals affected by a privacy breach.[38] Other state laws are similar to the California law.

[98] In California, a public sector agency and business that owns or holds computerized data that includes personal information must notify, within an expedient time, California residents of a security breach that results in acquisition of their personal information by an unauthorized person.

[99] The California law is aimed at reducing identity theft. For this reason, it defines personal information quite narrowly as including social security number, driver's licence number or California identification card number and financial account information (including credit or debit card numbers).

[100] The notification obligation does not apply to encrypted personal information.

[101] Nor does notification have to be individual where the cost of individual notification would exceed $250,000 or the number of individuals to be notified exceeds 500,000. In either case, substitute notification is permitted, through major statewide media, web posting and email where an affected individual has given an email address.

---

[37] I will leave it to another day to decide the question of whether the security measures obligation under s. 30 of FIPPA or s. 34 of PIPA in some cases will require notification of affected individuals. There are certainly good arguments to be made in favour of such an interpretation in certain circumstances.

[38] Civil Code, Sec. 1798.29 & 1798.82.

[102] As for privacy commissioners, at least one has suggested that, unless a case involving a privacy breach is exceptional, the responsible organization should notify those affected by the breach. Victorian Privacy Commissioner Paul Chadwick recently found that the Australian State of Victoria's Office of Police Integrity ("OPI")—a civilian oversight agency for police conduct—had inappropriately disclosed personal information from a database. The OPI had mistakenly mailed to a complainant a file that contained personal information of some 500 individuals and the file was in the complainant's hands for nine weeks before being returned to the OPI. Commissioner Chadwick's report merits careful consideration.

[103] As part of his investigation, the Commissioner considered whether the OPI should notify the affected individuals. He identified the applicable rule as Information Privacy Principle 4 (Data Security) under the *Information Privacy Act* of Australia's State of Victoria, which reads as follows:

> 4.1 An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.
>
> 4.2 An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

[104] Having found that the OPI breached its duty to protect personal information, Commissioner Chadwick started his analysis of whether affected individuals should be notified by saying that the "presumption is that privacy breaches ought to be notified to those whom they potentially affect."[39] He arrived at this presumption having considered the statement of purposes in the *Information Privacy Act*, which included the principle of transparency in the collection and handling of personal information. Commissioner Chadwick added, however, that in "exceptional circumstances, notification may be neither necessary nor desirable"[40] and went on to say this:

> In deciding whether the circumstances of any case are exceptional such as to make notification neither necessary nor desirable, the following factors should be considered in context by an appropriately senior decision maker in possession of the relevant facts –
>
> 1 The potential for reasonably foreseeable harm to result from the breach for the persons whose information is involved (referred to as the 'data subjects') or others affected, having regard to:
>
> - the nature of the information, in particular its sensitivity;
> - the amount of information;

[39] Para. 9.3.1, p. 65.
[40] Para. 9.3.3, p. 65.

- the extent of the unauthorised access, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, especially in mass media or online;
- any relationship between the recipient/s and the data subjects;
- the degree to which the data subjects may already be aware of the breach of their information privacy and be able themselves to minimise harm;
- the steps taken by the organisation to contain the breach and minimise harm.

2 The potential for notification itself to cause reasonably foreseeable harm to the data subjects (or any other person), excluding potential harm to those responsible for the breach (such as damage to reputation, or exposure to disciplinary action or claims for redress, or bad publicity).

3 Whether, considering 1 and 2, notification is reasonably likely to alleviate more harm than it would cause.

[105] Principle 4.1 under the *Information Privacy* Act uses language that is similar to that of s. 30 of FIPPA, quoted above.[41] Despite the similarities between s. 30 and Principle 4.1, I do not think that s. 30 of FIPPA, interpreted in its statutory context—including the purposes statement in s. 2 of FIPPA—was intended to establish any presumption that notification is required absent exceptional circumstances.[42]

[106] The above analysis from the Victoria report is, nonetheless, of assistance in assessing the situation under British Columbia law. I also consider that factors mentioned in the California law are of use in relation to British Columbia law. In my view, the key (but not sole) consideration overall should be whether notification is necessary in order to avoid or mitigate harm to an individual whose personal information has been disclosed. The harm-assessment approach, I note, has also been used by the Office of the Information and Privacy Commissioner for Alberta in investigations into personal information security breaches under Alberta's *Personal Information Protection Act*.[43]

[107] As indicated earlier, the 41 backup tapes were retrieved and returned to the government's custody. The evidence available to me suggests that the individual who bought them from AIR is in the business of acquiring and reselling used computer equipment and parts and that his purchase of the tapes was in the ordinary course of that business. At my request, he swore an affidavit in which he deposed that he had not made or kept any copies of the tapes or otherwise copied information on the tapes, including by saving or storing of

[41] It is also similar to the language of s. 34 of PIPA, quoted above.
[42] I will note here that British Columbia law has no explicit equivalent to Principle 4.2 under the *Information Privacy Act*.
[43] See, for example, Investigation Reports P2005-IR-001 and P2005-IR-002, www.oipc.ab.ca/ims/client/upload/P2005_IR_001.pdf www.oipc.ab.ca/ims/client/upload/P2005_IR_002.pdf.

computer data. He also swore that he had no personal knowledge of anyone else accessing the tapes or any information stored on them before they were delivered to *The Vancouver Sun*. The purchaser also swore that he had delivered all of the tapes to *The Vancouver Sun* around February 2006.

[108] For its part, *The Vancouver Sun* copied the personal information that it had used for its newspaper articles onto one DVD disc and three CD discs. Representatives of my office communicated with *The Vancouver Sun* and its representatives and ultimately we were satisfied with *The Vancouver Sun*'s proposal for securing those materials and its assurances as to security of the tapes and their contents while in its possession. Those assurances came in the form of an affidavit sworn by the Deputy Editor of *The Vancouver Sun*.

[109] There is no evidence or suggestion that, after the sale of the 41 tapes, any of the personal information on them has at any point been disclosed to, or possessed by, anyone other than the purchaser and *The Vancouver Sun*. There is very good reason to believe, and I conclude, that personal information has not been disclosed to or used by anyone other than the purchaser and *The Vancouver Sun*. The purchaser has sworn that the only thing he did with the personal information was provide it to *The Vancouver Sun*. In turn, *The Vancouver Sun* used the personal information for its newspaper articles and some information appeared in those articles (mostly but not entirely without direct identification of individuals involved). The copies of personal information that *The Vancouver Sun* retained have been put into safe-keeping.

[110] These circumstances weigh heavily against recommending that the government give notice to individuals whose personal information is on the tapes, either directly and individually or by substituted notice in a newspaper. As Commissioner Chadwick noted in his report, in assessing the risk of harm and notification, one should consider "the extent of the unauthorised access, use or disclosure, including the number of likely recipients and the risk of further access, use or disclosure, especially in mass media or online". In this case, the unauthorized disclosure was very limited and, *The Vancouver Sun* having stated that it intends to publish no more stories using the personal information, there is no realistic risk of further access, use or disclosure.

[111] Another consideration is that the publicity surrounding this matter means many if not all of the individuals whose personal information is on the tapes will be aware that their information is on the tapes, which are now back in government hands.

[112] Also, my office facilitated the return of the tapes to the provincial government, a step that helped contain the breach and minimise any risk of further harm due to the disclosure.

[113] Last, in light of the large number of individuals involved, and the fact that the information is some five years old, the cost to the provincial government of notifying individually or collectively would, it is reasonable to suggest, be considerable. I do not need to decide conclusively, however, to what degree if any the cost issue weighs against or for notification.

[114] This is because, in my view, notification in any form is not necessary to avoid or mitigate harm of any kind to the individuals whose personal information is involved here. The personal information disclosure here was very tightly contained (the purchaser of the tapes and other storage and *The Vancouver* Sun). Moreover, the personal information is back in government hands. There is no evidence of ongoing risk to individuals through identity theft or other harm. Notification is not necessary to address harm, past, present or future.

3.5 Recommendations

[115] As noted earlier, the risks for personal information security are constantly, and rapidly, evolving. Government has to stay on top of the risks and ensure that its security measures, and business rules and practices, reasonably respond to current and evolving risks. Moving forward, it will be necessary for government to ensure that it invests resources sufficient to ensure that the recommendations made below, and those found in the CIO's report, are properly implemented and to ensure that reasonable steps are taken to protect personal information at all times.

[116] The sharing of personal information across government and between public bodies is on the table as governments everywhere are increasingly looking to information technology to improve services and find efficiencies. Public trust and confidence in government's commitment to privacy, and to protecting personal information from security risks, will be lost if government cannot reasonably assure the public that meaningful investments are being made in personal information security at all levels.

[117] This case illustrates why the government's investments will have to address risks of human error, not just technological solutions for personal information security threats. After all, failures of personal information security are often failures of business practice, not information technology. As my colleague, Ontario Information and Privacy Commissioner Ann Cavoukian, observed late last year in her investigation report on a personal information security breach:

> …Many of the privacy breach incidents that have appeared in the headlines this year demonstrate a failure of business practices, not a failure of information technology.
>
> Many of the security breaches identified may have been avoided if simple physical safeguards had been in place and adhered to: computer databases that were physically lost or stolen in transit, hard drives

> physically removed from computers, laptops gone missing from sidewalks, taxicabs, hotel rooms. In many instances, physical access to the data or media is all that is needed for a privacy breach to take place.[44]

[118] In this light, and subject to what is said below, I agree with and support the recommendations made in the CIO's report on this matter.[45] The provincial government should move quickly to adopt and implement the CIO's recommendations as discussed here. I acknowledge that, as work proceeds, further steps may be identified and my office is committed to consulting with provincial government officials as they work to create new policies and procedures. The key is for the provincial government to move quickly and vigorously to address the immediate personal information security lapses identified here and to identify and remedy any other personal information security deficiencies it identifies system-wide.

[119] Some aspects of the CIO's recommendations require comment.

[120] First, the CIO's recommendations would continue to leave central policy direction to the Core Policy Manual (see recommendations 1 and 3, for example, and particularly recommendation 8). It would, however, leave individual ministries in charge of shaping local policy on the disposal of media. As the CIO's report indicates, though, MEIA did not have in place adequate policies and practices and the report also indicates that other provincial government ministries have failed to adopt and implement relevant policies despite their obligation to do so.

[121] In my view, a better approach would be for the CIO to review existing policy and then create a central policy with which all ministries and provincial government agencies must comply. This would include AIR, whose actions clearly played a role in the sale of the tapes. It would include clear rules and standards for destruction of storage media and devices and assign to one agency the responsibility for destruction.

[122] Oversight of compliance should be subject to monitoring by the CIO and to external audit and checking, by my office where necessary. The present situation, with individual ministries being responsible for their own policies and compliance, should not be allowed to continue.

[123] The central direction should cover all aspects of the lifecycle of media containing personal information, including in relation to office moves and to secure disposal of media containing personal information. As this report indicates, the disclosure of personal information in this case occurred due to

---

[44] Ontario Information and Privacy Commissioner, *Identity Theft Revisited: Security is Not Enough* (September 2005), pp. 20-21. http://www.ipc.on.ca/userfiles/page_attachments/idtheft-revisit.pdf.
[45] The CIO's recommendations are reproduced in Appendix A to this report.

inadequate policies, practices and training. More needs to be done to guard against similar incidents in the future.

[124] Second, the CIO's report recommends that the provincial government "consider the feasibility of encrypting government data on portable storage devices…and on backup storage devices." I believe the government must move quickly, and with high priority, with a strategy for encryption of personal information. It is likely necessary only to encrypt personal information that is sensitive and the breadth of the commitment to encryption will have to be addressed. It is clear, however, that encryption is a powerful and practical approach to personal information security and the government should pursue that avenue vigorously.[46] I recognize that government's information technology assets are unlikely to be homogenous in terms of operating systems or age and that, for these and other valid reasons, an encryption solution will not appear overnight. Still, meaningful resources should be committed to such an effort with high priority.

[125] Third, the CIO's recommendations are aimed at the provincial government. Although it should go without saying, the government must ensure that all service providers under outsourcing or alternative service delivery arrangements use information technology security measures, and operate under policies and procedures, at least as good as those that the government employs. Regardless of the obligation of service providers for personal information security, the government at the end of the day remains responsible under FIPPA for the adequacy of security measures.

[126] I made this point in a January 21, 2002 letter to ministers regarding alternative service delivery and privacy protection. In addition to ensuring that privacy compliance is addressed in such arrangements, ministries should also ensure that they commit the resources necessary to monitor service provider compliance and should commit to enforcing their contractual rights when service providers fail to live up to their promises around personal information.

4.0 CONCLUSION

[127] As this report indicates, simple mistakes made in good faith by individual government employees resulted in unauthorized disclosure of highly sensitive personal information of thousands of British Columbia residents. We have no choice in the matter when government collects or compiles our personal information and in return British Columbia law requires public bodies to act

[46] As noted above, US privacy breach notification laws recognize the efficacy of encryption in protecting personal information, since they generally exempt agencies and organizations from any duty to notify individuals of disclosure of information where it has been encrypted. Also, US law requires federal government agencies to identify which personal information is sensitive and to encrypt it. See, for historical comparison, the *Computer Security Act of* 1987 http://www.nist.gov/cfo/legislation/Public%20Law%20100-235.pdf. More recently, see Title III of the *Federal Information Security Act* of 2002 http://csrc.nist.gov/policies/FISMA-final.pdf.

reasonably to protect our personal information. I accept that what happened here was an accident, but the systemic failures identified in this report, and in the CIO's report, need to be corrected as soon as possible. Personal information security is a serious matter and the provincial government needs to commit resources and energy to restoring and then retaining public trust in the government's handling of our personal information.

March 31, 2006

ORIGINAL SIGNED BY

David Loukidelis
Information and Privacy Commissioner
for British Columbia

OIPC File No. F06-28080

RECOMMENDATIONS IN CIO REPORT

Central Authority Accountability

1. It is recommended that government undertake a review of corporate asset management policies, procedures, standards and practices.

   The CIO, in collaboration with the Comptroller General, should review and amend asset management policies to improve tracking of the increasing array of information technology devices across government. This investigation has highlighted the need for policy that considers not just the financial value of assets but the value of and risk to the information assets that may reside upon/within them (a $40 tape holding the personal information of thousands of British Columbians). Specific consideration should be given to the areas of compliance review and audit methods, procedural checks and balances, as well as education and training.

   This review should also determine an appropriate method to implement an inventory management system for data storage media. This should include the classification of the information and the labelling and inventorying of the device.

2. It is recommended that an external process for ensuring ministry compliance with information management policy be developed, including but not limited to, spot audits.

3. It is recommended that Government assign authority to the CIO to "shut down" asset disposal at any ministry identified as non-compliant with CPPM, or where, in the judgement of the CIO local procedures are insufficient to protect personal information from accidental release.

4. It is recommended that government continue the current ban on the sale of all media storage devices. Government should ensure that the list of what is banned is comprehensive, complete and regularly updated and is communicated to all necessary parties.

5. It is recommended that government consider the feasibility of encrypting government data on portable storage devices (e.g., Blackberrys™, laptops, etc.) and on backup storage devices.

6. It is recommended that government update policy to include the reporting of lost portable storage devices, including storage media, (e.g., thumb drives, memory cards) regardless of financial value, within 24 hours from the time of loss.

   This policy, in conjunction with new encryption practices, can mitigate the risk to government information in portable devices.

7. It is recommended that government issue policy that all computer files containing personal information be stored on the government network and not on "non-encrypted" personal computing devices or data storage media (e.g., personal computer hard drives, laptops, PDAs, etc.).

Ministry Accountability

8. It is recommended that ministries conduct a comprehensive review of how ministry policies, procedures and processes for the disposal (including destruction) of computer assets are implemented in support of ministry accountability under the Core Policy and Procedures Manual.

   Additional training should be provided for all staff that have care or control of personal or sensitive information including disposal.

Ministries should designate a senior management position responsible for regular inspection and reporting regarding ministry compliance with all relevant legislation and policy related to the protection of personal or sensitive information.

Ministries should develop and communicate policy that explicitly states that managers who delegate responsibility for final sign-off on disposal or sale of any device or media covered under either the interim or the permanent ban are responsible for any actions taken by those to whom they delegate, including contractors or subordinates.

Ministries should conduct regular internal audits to ensure compliance with information management policy and must immediately address any deficiencies that are identified through either internal or external audits.

Specific documentation templates, procedures and accountabilities should be developed to ensure verification that no data storage media are included in any lots disposed by AIR. This includes non computer equipment lots.

9. It is recommended that the management responsible at the two ministries involved in this incident (Ministry of Employment and Income Assistance and Ministry of Labour and Citizens' Services, Asset Investment Recovery Unit), identify the gaps in procedures and processes that resulted in non-compliance to policy. This will also include actions to immediately address these gaps.

Personal Accountability

10. It is recommended that government conduct a comprehensive review of current personal and management accountability mechanisms for all individuals involved in handling, labelling, storing or disposing of sensitive media or devices.

    This should include the development and implementation of personnel policy that clearly outlines the individual accountability of all public servants who are required to handle, label or dispose of sensitive media or storage devices.