

PRIVACY BREACH HUMAN RESOURCES REVIEW

*Ministry of Children and Family Development
Ministry of Housing and Social Development
BC Public Service Agency*

JANUARY 2010

Review conducted by:
Bert Phipps
Assistant Deputy Minister
Ministry of Public Safety and Solicitor General

CONTENTS

EXECUTIVE SUMMARY	3
ACKNOWLEDGEMENTS	4
BACKGROUND	5
KEY EVENTS CHRONOLOGY	7
MAJOR AGENCIES INVOLVED	10
FINDINGS OF FACT	14
FINDINGS ABOUT POLICY, PRACTICE AND JUDGEMENT	16
RECOMMENDATIONS	23
APPENDIX A	26
APPENDIX B	28
APPENDIX C	30
APPENDIX D	31

EXECUTIVE SUMMARY

On April 7, 2009 an employee of the Ministry of Children and Family Development (MCFD) was arrested in the workplace and a search warrant was subsequently executed at his home. Documents were found at the home containing personal information about clients of government services, along with equipment which could be used to fabricate identification. Later, it was learned by MCFD that the employee had a criminal record. More than six months later, the employee was dismissed. His spouse, employed by the BC Public Service Agency, was dismissed shortly afterwards.

On December 4, 2009, two reviews were announced by government. One would determine what happened with respect to the privacy breach, and the other, a human resources review, would examine the management of the employee. Both would consider how situations like this might be prevented.

In the course of the review of human resource issues seventy hours of interviews were conducted and over one thousand pages of documents were reviewed. A chronology of events was developed. The analysis of this information resulted in nine findings about human resource issues.

In summary, the review found the difficulties began with the employee's deception about his criminal and employment history, when he was hired by the Ministry of Employment and Income Assistance in 2006. In the course of two and a half years of employment with two different ministries, he accumulated a number of documents containing personal information in his home, and while this presented a serious risk, there is no evidence to date that the documents were used for criminal purposes. The employee and his spouse were appropriately dismissed from the public service, but the road to this conclusion was unnecessarily long and circuitous. No one, other than the employee, acted in bad faith, but there were a number of examples of poor judgement by government officials, which worked against a timely and effective response. Some organizational and cultural factors influenced the judgement exercised, and these merit further attention.

No criminal charges have yet been laid in this case, but criminal investigations are continuing.

Based on the findings, six recommendations are made to help avoid similar events:

1. The BC Public Service Criminal Records Check Policy should be reviewed, in consultation with the Government Chief Information Officer, with an eye to expanding the types of positions which are considered for designation as subject to a criminal records check. In particular, positions which provide access to personal information systems should be considered.
2. In the longer term, as technology advances, the BC Public Service Agency and the Ministry of Public Safety and Solicitor General, should explore ways to enhance the thoroughness and integrity of background checks.
3. A new human resource policy should be introduced to complement the current Criminal Records Check Policy. This new policy would mandate the steps to be taken when a government employee is arrested, charged, or convicted of a criminal offence.
4. The Ministry of Children and Family Development and the BC Public Service Agency should confirm the transition plan for human resource services, to ensure clarity in the respective roles and responsibilities of Strategic Human Resources and the BC Public Service Agency.
5. Following a review of this report, and the companion report on the privacy breach, the Ministry of Children and Family Development should review the judgement exercised by the managers involved and identify remedial action to ensure managers have the direction, training and support to respond more effectively to complex issues.
6. The Deputy Ministers' Council should review how external investigative agencies link with government when public servants are the subject of a criminal investigation. The aim of the review would be to ensure that the right information gets to the right people in government in a timely manner, while simplifying the process for police and other enforcement agencies.

ACKNOWLEDGEMENTS

The co-operation of many people and agencies assisted in the timely completion of this review. Staff members in the public service made themselves readily available for interviews, and were helpful and open in answering questions and providing documents. Outside the government, the Royal Canadian Mounted Police, and other investigatory agencies, were generous with their time and expertise. Finally, the deputy ministers in the involved ministries have been fully supportive of an unfettered review, and are interested in enhancing policies and practices based on the conclusions of this review.

BACKGROUND

This report is the result of unusual events which took place in government during 2009; what was subsequently learned about the government employee at the centre of those events; and the actions taken, or not taken, by other government staff in response to this information.

On April 7, 2009 an employee of the Ministry of Children and Family Development was arrested in the workplace by the RCMP Commercial Crime Section. He was brought to the attention of police because of concern by ICBC's Special Investigation Unit that the employee possessed two drivers' licenses under different surnames. On the same day, the police executed a search warrant at his home and located 408 pages of government documents containing personal information about clients of government services. They also found some equipment which had the potential to be used to fabricate false identification (a scanner, a laminator, and three computers). The employee also had a criminal record for various offences related to fraud, a fact not known by government when he was hired in 2006. More than six months after his arrest, the employee was dismissed from the public service. His wife, who also worked in government, was dismissed shortly after. To date, no evidence has been found to suggest that the employee used the information he possessed for any criminal purpose.

In British Columbia, the protection of personal information held by provincial government agencies is governed by the *Freedom of Information and Protection of Privacy Act*, and by policies and practices adopted in ministries and agencies throughout the province. Many conscientious public servants take work home, and some work from home on a regular basis. Provided the relevant policies are followed to keep personal information secure, the practice does not violate the Act or cause significant concern. In this instance, however, clients' personal information was found in the home of an employee who had two drivers' licenses, who had misled the employer about his history of fraud-related activity, and who also possessed equipment which might be used to fabricate identification. This elevated the risk level significantly. The public would naturally want to know how the situation came about, whether the response by government officials was appropriate and timely, and how a recurrence of the situation could be avoided.

On December 4, 2009, Citizens' Services Minister Ben Stewart announced two reviews into this case, with the reports to be made public. The first review would examine how policies and practices for the protection of personal information were applied in this case, and how government responded when it appeared that the privacy of some citizens had been compromised. This review has been carried out by the Office of the Government Chief Information Officer, Ministry of Citizens' Services, which has responsibility for information and privacy policies within the provincial government.

The second review would examine how human resource (personnel) policies and practices were employed in the case. To bring objectivity to this review, the Head of the Public Service Agency directed that it be conducted by a person outside the Ministry of Children and Family Development (MCFD), the Ministry of Housing and Social Development (MHSD) and the BC Public Service Agency (BCPSA). Assistant Deputy Minister Bert Phipps, of the Ministry of Public Safety and Solicitor General, was selected for this assignment.

The privacy breach review will determine how the breach occurred, examine the adequacy of the government's privacy breach protocol, and identify opportunities to improve government's information security, access, and file storage and management practices.

The specific objectives of the human resource (HR) review are to:

- Identify the various parties that were involved in the human resource processes and decisions.
- Confirm the events and facts pertaining and relevant to the human resource processes.
- Assess the human resource policies, practices and judgement applied by those individuals.
- Identify where improvement is required in existing policies, the application of those policies or in the operating principles and practices of HR and management staff in managing these types of matters.

While the two reviews have independently arrived at their findings and recommendations, they did share information, and created a common chronology.

This report endeavours to include all the information relevant to its findings and recommendations. There are some challenges in accomplishing this. As the Minister committed to release it publically, the report must comply with the privacy provisions of the *Freedom of Information and Protection of Privacy Act*. Secondly, as outside investigations are still continuing into these matters, it is critical that the report not compromise those investigations or any resulting proceedings.

KEY EVENTS CHRONOLOGY

This chronology captures the major events in this case. There were, in fact, numerous telephone calls, emails, and meetings about this employee and his spouse between March and November 2009, including periods when no activity is evident in this chronology. This summary only includes events which represented a significant turning point in the case, or which are needed to understand the essentials of the case. This summary concludes with the notification of the Minister and Deputy Ministers, and the dismissal of the employees. The companion report on the privacy breach contains additional chronology entries in October, November and December 2009, which are relevant to that review.

1993.08.23	Employee is hired by (then) Ministry of Social Services as a Financial Assistance Worker, and subsequently moves to another position in the Ministry of Health.
2002.04.01	Ministry of Health position is transferred to the new Interior Health Authority. He is dismissed from this position on September 10 th , 2003.
2005.04.22	Convicted in Kamloops of theft, unauthorized use of credit card data, possession of stolen property, possession of counterfeit money, and uttering or using counterfeit money.
2006.10.02	Submits a criminal record check form to RCMP and has it returned (still under investigation).
2006.10.16	Hired by the (then) Ministry of Employment and Income Assistance as an auxiliary Employment and Assistance Worker.
2007.09.14	Following positive references, wins a competition for a regular position as an Administrative Officer in the Ministry of Children and Family Development, Provincial Children and Youth with Special Needs Operations (PCYSNO). Gains recognition as an excellent employee.
2008.06.23	Ministry of Employment and Income Assistance (MEIA) becomes part of new Ministry of Housing and Social Development (MHSD).
2009.02.26	ICBC Special Investigation Unit makes first contact with Government Security Office (GSO), of the Ministry of Finance's Risk Management Branch regarding an investigation of driver's licenses held by a government employee.
2009.04.06	RCMP liaises with GSO regarding their investigation.

2009.04.07	RCMP Commercial Crime Section and Victoria Police arrest employee at work and search his home, seizing documents and equipment. Employee is released without charge that evening. Employee's access to government computer systems is revoked.
2009.04.08	Senior Director of PCYSNO calls police to ask if there is any risk to the ministry. Police only confirm that the matter concerns drivers' licenses, and that ministry staff need to make their own assessment of risk.
2009.04.08 - 27	Employee is absent from work, initially at direction of employer, and later because of illness.
2009.04.09	Police provide GSO with a one-page sample of the government documents they seized during the search. Sample is subsequently shared with MCFD Strategic HR.
2009.04.14	Strategic HR and the employee's manager discuss the sample document. Initial response from employee's manager is that having these documents at home is consistent with the employee's duties.
2009.04.27	Employee returns to work. Access to systems is restored with manager monitoring the employee's activity.
2009.05.20	Senior director PCYSNO and BCPSA human resource consultant conduct an investigative interview with employee in the presence of his shop steward. They are satisfied with his answers about his identity and driver's licenses, but give him a verbal reprimand for studying for a university course while on government time (an issue that came to light during their investigation).
2009.07.09	Police advise GSO that their investigation to date, using a sampling of the personal information found in the home, has revealed no evidence that the employee used any of the information in his possession for purposes of fraud or identity theft. Their investigation into other issues continues.
2009.07.14	Police turn over all seized government documents to an MCFD information security officer. There are nine different types of documents, comprising 408 pages in all (based on information from GCIO). MCFD determines that the bulk of the material (8 categories) originates with MEIA and dates from the period December 2006 to March 2007. Remaining documents are from a shared MCFD/MEIA database and date from March to September 2008. Police also advise that the employee: has a criminal record for several fraud-related offences; the criminal record check submitted by the employee requires further investigation; and the employee's spouse is employed in government.

2009.07.20	MCFD shows documents to Information Access Operations (IAO) staff members located at MHSD, who recognize potential privacy breach. They recommend that the breach be reported to the Office of the Information and Privacy Commissioner.
2009.07.22	MCFD turns over the MHSD (formerly MEIA) documents to that ministry.
2009.07.27	<ul style="list-style-type: none">• Prevention and Loss Management Services (PLMS) of MHSD commences its investigation.• Employee's manager meets with MCFD information security officer and Strategic HR representative to review the case. Other information provided by police on July 14th is shared.• MCFD manager meets with employee to discuss why he had the shared database documents at home and is satisfied that he required them for work purposes.
2009.08.13	PLMS delivers the documents found in the home to IAO staff.
2009.08.14	PLMS investigation becomes a criminal investigation in concert with RCMP.
2009.08.24	PCYSNO Senior director MCFD contacts police to ask about status of investigation and whether precautions are required. Police reply that investigation is ongoing in partnership with PLMS, and that advice on precautions should come from MCFD information security staff.
2009.08.25	PLMS contacts BCPSA to advise that investigation is ongoing and BCPSA will be advised when it is concluded.
2009.10.15	PLMS briefs MCFD senior director and BCPSA human resources consultant about findings of their investigation to date, regarding identity and criminal record. They, in turn, brief MCFD Senior Executive Director. Decision is taken to suspend employee without pay pending further investigation. Employee's systems access revoked.
2009.10.16	Employee is suspended without pay pending investigation. Managers in BCPSA suspend employee's spouse without pay pending investigation.
2009.10.20	Head of the BCPSA informs the Minister of Citizens' Services of the case. This is his first knowledge of the case.
2009.10.21	Head of the BCPSA informs the Deputy Minister of Citizens' Services, the Deputy Minister of MCFD and the Deputy Minister of MHSD about the case. This is their first knowledge of the matter.
2009.10.22	Employee is dismissed from the public service.
2009.11.13	Employee's spouse is dismissed from the public service.

MAJOR AGENCIES INVOLVED

MINISTRY OF CHILDREN AND FAMILY DEVELOPMENT (MCFD)

The Ministry of Children and Family Development has approximately 4500 FTEs (full time equivalents) and a budget of over \$1.3 billion. This large ministry delivers a diverse range of services, including child protection, youth justice, adoptions, child care, early childhood development and child and youth mental health. Three of its many branches were involved in this case.

Provincial Children and Youth with Special Needs Operations (PCYSNO)

There are four components to this branch. One of these is the Medical Benefits program, which funds medical equipment and supplies for severely handicapped children, as well as optical and medical benefits for children in care. The employee in question supervised one of two sub-units within the Medical Benefits component. Staff members in this unit do not work directly with children, but in the course of approving and processing payments, they require access to personal information about clients, including names, dates of birth, addresses, provincial health numbers and social insurance numbers. The two supervisors, who are union members, report to a manager excluded from union membership, who reports to a senior director responsible for the entire PCYSNO branch. This person, in turn, reported to an Assistant Deputy Minister responsible for Provincial Services (as part of a larger organizational change, PCYSNO now reports to a different ADM).

Strategic Human Resources (Strategic HR)

Human resource work within the public service is generally divided into two categories. The first comprises transactional and employee relations support to staff and managers for such matters as hiring, promotion, attendance management, discipline, and grievances. In most parts of government, this support is provided by the BCPSA. The second category is strategic human resources, which is concerned with workforce planning, employee engagement and organizational development. Strategic HR offices are located in each ministry. In most instances, ministry staff who work in Strategic HR do not deal with specific employees, but with the workforce as a whole. MCFD was unique within government in that, during the time of these events, Strategic HR was still dealing with some employee relations issues.

Ministry Chief Information Officer (MCIO)

Each ministry has a Ministry Chief Information Officer who is responsible for information management and information technology within the ministry, including records management,

security, electronic service delivery and operational initiatives which are specific to the ministry. The Ministry Chief Information Officers (MCIOs) sit on the Government Chief Information Officer's Council to address cross-government policy and planning (see Government Chief Information Officer below). Employed within the MCIO's office was the Ministry Information Security Officer, who played an active role in this case.

MINISTRY OF CITIZENS' SERVICES (MCS)

The Ministry of Citizens' Services manages one of the most diverse portfolios in government, including the BC Public Service Agency, the Public Affairs Bureau, Enquiry BC, BC Bid, BC Stats, the Office of the Government Chief Information Officer, and Shared Services BC, which supports other parts of government by processing information requests, and supplying accommodation and technology. Three of its components were involved in this case.

BC Public Service Agency (BCPSA)

The Agency was formed in 2003 and is a "shared service" which provides human resource services to all parts of government. Although housed in MCS, it is accountable to the Province's Deputy Ministers Council. The agency has a range of human resources expertise, but most of its work is "transactional" in nature: providing support to staff and managers in ministries for classification of positions, recruitment, promotion, performance management, employee illness and injuries, discipline and grievances.

Government Chief Information Officer (GCIO)

The Government Chief Information Officer (GCIO) is the governance authority for standards, oversight and approvals for the Province's information and communications technology. As government's chief information and technology strategist, the GCIO is responsible for promoting and guiding the effective management of government information. The GCIO is responsible for government-wide policy, procedures and standards related to data access, privacy, records management, security and electronic service delivery. The GCIO also leads strategic planning for information management and technology and develops mechanisms to ensure compliance with government-wide policies.

Information Access Operations, Shared Services BC (IAO)

IAO is the operational arm of government which fulfills obligations under the *Freedom of Information and Protection of Privacy Act* and the *Document Disposal Act*. When citizens request information under the *FOIPPA*, staff in this office process the request. Previously, each

ministry in government had its own information and privacy section. During 2009, they were brought together in IAO.

MINISTRY OF FINANCE

This Ministry has about 800 FTEs and a budget of approximately \$90 million. One small unit within the ministry was involved in these events.

Government Security Office (GSO)

This office was created in 1995 and is located in the Risk Management Branch. It seeks to reduce opportunities for harm to the people, assets and operations of government. It is one component of a larger “enterprise risk management” discipline which identifies and mitigates risks across government. They promote harmonized policies and programs for security; provide advice and consultation; and broker information on successful risk mitigation. The two staff members are appointed as special constables, and have experience in policing, military service, intelligence, loss prevention and security.

MINISTRY OF HOUSING AND SOCIAL DEVELOPMENT (MHSD)

The Ministry of Housing and Social Development is a large, multi-faceted ministry created in 2008 to deliver employment and income assistance services, housing and homelessness strategies, labour market services, gaming policy and enforcement, and liquor control and licensing. It has approximately 2,600 employees and a budget of \$2.7 billion. Two of the Ministry’s components were involved in this case.

Employment and Assistance program

This component, largely inherited from the former MEIA, helps people move from income assistance to sustainable employment, and provides income assistance to people unable to fully participate in the workforce. Employment and Assistance Workers meet directly with clients to determine their eligibility for services, authorize payments, and direct them to employment and other services which will enable them to lead more independent lives. These services are provided in the Regional Services Division of the ministry. The employee in question in this review was employed from 2006 to 2007 as an Employment and Assistance Worker, and acquired most of the documents found in his home during this time.

Prevention and Loss Management Services (PLMS)

This branch is also located in the Regional Services Division of the MHSD, and is responsible for program integrity and loss management throughout the ministry. Their work is largely concerned with overpayments, and fraud allegations against those in receipt of ministry benefits. Ministry investigators also conduct certain internal investigations. About twenty investigators are designated special constables, and have legislated authority to share information with police for law enforcement purposes.

FINDINGS OF FACT

- 1. The employee deceived the public service when he applied for work with the Ministry of Employment and Income Assistance in 2006. If he had been truthful he would not have been hired.**

During the time he had been out of the public service (2003 – 2006), the employee had acquired a criminal record for offences relating to theft and fraud. Without providing specifics, as the matter is still the subject of investigation, he exploited weaknesses in the criminal record check process which was in place in 2006. Had his criminal record been known at that time, he would not have been employed as an Employment and Assistance Worker, which gave him direct access to clients and to personal information about a large number of ministry clients.

Material regarding reference checks completed in 2006 could not be examined as it has been destroyed in accordance with routine records destruction schedules.

The Public Service Criminal Record Check Policy was strengthened considerably, effective March 1, 2009, particularly with respect to the process of conducting criminal record checks (see appendices C and D).

- 2. The position the employee won by competition in September 2007 in the Ministry of Children and Family Development does not require a criminal record check.**

The very positive reference the employee received for his work at the MEIA helped him secure a regular position in MCFD. He also received a very positive reference from a provincial coordinator who supervised him during his tenure with the Ministry of Health. However, this person had supervised him until 2001, prior to the employee's transfer to the Interior Health Authority. Furthermore, on his 2007 application form the employee stated he had left his health position in July 2003 in order to pursue self employment. It is now known that he was dismissed from that position in September 2003.

With respect to criminal record checks, had he applied from outside the public service, or from a position within the public service which was not subject to a criminal record check, there would have been no criminal record check on file and none required. While the MCFD position does not involve direct contact with children or other clients, it does provide access to large amounts of personal information. The March 2009 revision of the Public Service Criminal Record Check Policy introduced many improvements. It attempts to strike a balance between the privacy of public service applicants and the need to

protect the public and their personal information. While it does not preclude positions like those occupied by the employee being designated as subject to a criminal record check, this is not the type of position specifically identified as requiring consideration for designation (see appendices C and D).

- 3. The documents found in the employee's home were acquired between October 2006 and September 2008, reflecting access he had to personal information both as a Ministry of Employment and Income Assistance employee and a Ministry of Children and Family Development employee.**

Between October 2006 and September 2007, while employed by MEIA, the employee obtained 378 pages of document printouts. These were documents he could access in the ordinary course of his work as an Employment and Assistance Worker. There was no reason for him to have these documents at home. A further 30 pages of document printouts were acquired while he worked at MCFD. These were also legitimately obtained in the course of his duties, but as with the MEIA documents, there was no reason to have them at his residence.

- 4. Through checking a sampling of the personal information found in the employee's home, the RCMP report there is no evidence to date that the documents acquired by the employee since 2006 were used for criminal purposes. There is likely no substantive harm to the public, but personal information was potentially at risk of criminal exploitation, and the affected parties were caused unnecessary concern.**

It is impossible to say conclusively what the employee's intentions were with respect to the personal information found in his home. Nonetheless, the material has now been returned to government, and there is no evidence to date that it was used for criminal purposes. While this is a relief to all concerned, the exposure of the personal information to possible criminal use is unacceptable, and no doubt caused the affected citizens some anxiety that was unnecessary and regrettable.

FINDINGS ABOUT POLICY, PRACTICE AND JUDGEMENT

- 5. While still subject to the collective agreement grievance process, this review finds that the termination of the employee was appropriate.**

Although it took an unnecessarily long time for events to unfold, the final decision to terminate the employee was the appropriate outcome. By his deliberate deception at the time of his employment in 2006 the employee breached the trust which must exist between employer and employee. The employment relationship was irrevocably damaged and his continued employment could not be supported.

- 6. This review finds that the termination of the employee's spouse was appropriate.**

There is no evidence that the employee's spouse was party to the collection of government documents at home, or any deception about her husband's criminal record. As an employee of the BCPSA; however, she had access to highly confidential employee information. The arrest of a close family member, also a public servant, and the search of their common home, was a relevant and serious situation which she should have reported to her employer. Steps could then be taken to preserve the integrity of the BCPSA, which would invariably be involved in dealing with the allegations against her husband. This would have ensured that no conflict of interest occurred.

The employee's spouse was excluded from union membership, as are all BCPSA employees. She had the benefit of counsel during the disciplinary investigation. A review of the relevant documentation, including the notes from the interview with the employee, leads this review to conclude that there was an irreparable breach in the employer – employee relationship.

- 7. The combination of circumstances in this case was highly unusual, and would be outside the experience and training of many government managers.**

This case involved criminal investigations by enforcement agencies (still not concluded), a government labour relations investigation, and a government response to a possible privacy breach. In addition, some of the events in question occurred in one ministry, while the employee was working in another. Finally the employee had gone to considerable lengths to conceal his employment and criminal history, which had occurred in another part of the province. Many public servants became involved in responding to

these events. In all, there were twenty-six officials, in a number of divisions, within four different ministries, who had more than fleeting contact with these events.

Most managers in government will go through their entire careers without ever having an employee investigated by the police. When the other complicating factors are added, this case stands as an unusual confluence of circumstances. It is not beyond the capacity of government to competently manage a case like this, but that management requires a higher degree of co-ordination, communication and resolve than occurred in this case.

8. No human resource policies were violated, and apart from the employee, no one acted in bad faith, but the judgement exercised in many instances in this case fell short of the due diligence which is expected in government.

A review of recruitment, criminal record check, and labour relations policies in effect at the time of these events reveals no violations of policy. Similarly, there is no evidence that any personnel in MCFD, MEIA, MHSD or the BCPSA, save for the employee, acted in bad faith. However, the response to the police actions and the information which became known about the employee was significantly inadequate, both in terms of timeliness and concern for protection of privacy. The failings observed during this review can be roughly characterized under three headings:

- A. Missed opportunities at critical junctures;
- B. Information dead-ends; and
- C. Unconfirmed assumptions.

A. MISSED OPPORTUNITIES AT CRITICAL JUNCTURES

Return to work of the employee on April 27, 2009

After his arrest on April 7th the employee was absent from the workplace for ten days, initially at the request of the employer, and later due to illness. When he returned on April 27, 2009 his access to systems was restored, but under closer monitoring by his manager. The police had been circumspect to this point about their investigation. However, there were sufficient red flags that he should not have returned without a thorough investigative interview, in the presence of a shop steward. The managers responsible for him did not have enough detail about the situation in order to make an informed decision about his return to that position. They relied primarily on their perception of him as a diligent employee. They should have sought more information

from the employee, the GSO and the police, and made more enquiries about the sample document which the police had provided.

Investigative interview on May 20, 2009

The interview conducted on May 20th contributed little new information about the employee's identity, his past troubles, or his possession of documents at home. Investigation prior to the interview had revealed that he had been studying for a university course on government time, and this became the focus of the interview in the minds of both the BCPSA and MCFD interviewers. Other issues received scant attention. Those interviewing him demonstrated a regrettable lack of curiosity about his past, and reluctance to ask probing questions. When the employee provided openings to this part of his life in the interview, they declined to pursue the line of questioning. They felt obliged to confine their enquiries to the pre-formulated questions.

Enquiry made to police on August 24th

A senior director in MCFD contacted the police on August 24th to ask about the status of the investigation, and whether they should be taking any precautions with respect to the employee. The police replied that their investigation was ongoing and being conducted in partnership with the PLMS in MHSD. With respect to precautions, the police suggested the director should be taking advice from the ministry, and in particular the information security official who had been involved earlier. It does not appear that the director made contact with either PLMS or the information security official.

B. INFORMATION DEAD-ENDS

Police information retained at Government Security Office

Prior to and immediately following the employee's arrest and the search of his home, police and the ICBC Special Investigation Unit provided information to the GSO of the Ministry of Finance's Risk Management Branch, whose staff have special constable status. Some of this information was provided in confidence, and the GSO was respectful of that stipulation. Police were connected by GSO with the appropriate MCFD officials to effect the arrest of the employee and make other enquires. GSO staff acted within their mandate and did not share confidential information with ministry managers. In other words, one part of government had the information, but not in a form in which key pieces could be conveyed to other parts of government, particularly to managers who were responsible for the employee at the centre of the events. There appears to have been no mechanism by which Risk Management Branch (Government Security Office) could help

managers assess and mitigate the risk posed by the employee, and at the same time maintain their special relationship with the police.

Meeting to review evidence on July 27th

The manager, and a Strategic HR representative, met with the MCFD information security officer, and discussed what was known about the case. The information security officer had met with the RCMP on July 14th, and they had turned over all the documents they had seized at the employee's home. The officer reported that the employee had a criminal record for creating false identification, that there was concern about the criminal record check provided to government, and that the employee's spouse also worked for government. Little action resulted from this meeting. The manager did ask the employee why he had the documents at home, and was satisfied that he required them for work purposes. No one escalated the information reported at the meeting to any higher authority. The information security officer tried to, but was told by the officer's supervisor that this was the responsibility of the program area. It is clear that senior managers in MCFD's Provincial Services Division would have viewed the labour relations issues much differently had this information been conveyed to them by the employee's manager, the information security officer or Strategic HR. As it transpired, the senior managers did not hear about these elements until mid October.

Briefing notes prepared by Prevention and Loss Management Services, Ministry of Housing and Social Development

A thorough investigation was commenced July 27th by an investigator within PLMS, who had special constable status. Briefing notes about progress made in the investigation were prepared regularly: on August 4th, August 18th, and August 26th. The investigator had met with the police and these briefing notes conveyed information about the identities of the employee, his criminal record, concerns about the criminal record check, the variety of documents found in his home, and the employee's spouse. None of these briefing notes was shared with MCFD, where the employee continued to work. MHSD did advise the BCPSA in early September that an investigation was underway and the agency would be advised when it was concluded. However, the important information which would have been of immediate value to those responsible for managing the employee was not communicated.

C. UNCONFIRMED ASSUMPTIONS

There were several occasions between April and November 2009 when public servants assumed that someone else already knew about a critical piece of information, or that certain information was reliable. They did not confirm their understandings and as a result the timeframe for action was unnecessarily extended.

MCFD examination of the sample document

The employee's managers were told in April about the sample document which was representative of those found in the employee's home, and assumed that if he had them there, he must have required them for a legitimate work purpose. No serious effort was made before July to match specific documents with specific work assignments.

The employee's truthfulness

The managers responsible for the employee assumed that a person who presented as earnest and hardworking would answer their questions truthfully and volunteer any relevant information to them. With most well performing employees, this is a safe assumption. While the employee did, in fact, volunteer that he was trying to distance himself from his past, they assumed that past had no bearing on his current employment. Even after learning in July of the criminal record and concerns about the criminal record check, the employee's manager maintained that the employee was highly professional, performed beyond the call of duty, and should be supported.

Knowledge that the employee's spouse worked at BCPSA

This was evidently common knowledge among a number of people in BCPSA and MCFD. They assumed it was known by senior people in BCPSA. In fact, they were not apprised of this information until October.

The role of the program managers

Staff in MCFD's Strategic HR office assumed that the program managers would deal with the information learned at the July 27th meeting about the employee's criminal record and the suspect criminal record check. Within Strategic HR, one member wrote an email to another expressing grave concern about the potential for criminal activity in this situation, and offered the opinion that the case should be referred to the BCPSA's Labour Relations unit. Neither colleague took any further action because they thought the matter was the responsibility of managers in PCYSNO.

The role of Strategic HR

MCFD's information security officer assumed that MCFD Strategic HR was actively managing this case. To the officer's credit, this assumption was eventually checked out with an email on September 30th. It was discovered that Strategic HR staff were playing a passive role at that time, waiting to hear from others about the case.

Communication between MCFD and police

The senior director in MCFD assumed in August that if police knew something that would be of concern to MCFD, this would be conveyed to the director. This director was unaware of the information already provided by the police to the ministry information security official and subsequently to the employee's manager in July (while the senior director was on holiday). As a result he felt no need to contact the PLMS investigator, when the police advised they were working with that unit.

Communication between MHSD and MCFD

An executive member of MHSD reviewed the August 26th briefing note prepared by PLMS upon return from holiday in September, but this person's attention was diverted by pressing operational matters. The executive assumed that MCFD was being consulted, but that was not the case (the executive filed the document without sharing its content with the Deputy Minister).

- 9. There were a number of organizational and cultural factors which contributed to the failings in judgement noted above.**

Organizational and Personnel Changes

The Strategic HR section in MCFD was in the process of narrowing its role to the workforce planning, employee engagement and organizational development functions typically associated with strategic human resources. The BCPSA was assuming greater responsibility for day-to-day personnel issues in MCFD. BCPSA, Strategic HR and program staff indicated they understood their roles and responsibilities, but to the external eyes of this review, the shifting leadership of this case among BCPSA, Strategic HR, and the program managers, does not appear to have followed any plan or mutual agreement.

The information and privacy staff attached to MHSD were in the midst of a transition when they became involved with the documents during the summer of 2009. There were changes in personnel and a portion of their attention was focused on the transition. Whereas they had formerly been employees of the MHSD, they were moving to

Information Access Operations in MCS. While their physical location remained the same, their accountability was changed to the new information access entity.

It should be noted that the senior director in PCYSNO had started in the position only four days prior to the employee's arrest, and two of the BCPSA consultants involved had only been in their positions for three months. This was a particularly complex and demanding case to be managed by staff members who were relatively inexperienced in their positions.

Culture of Privacy – Unintended Consequences

The introduction of the *Freedom of Information and Protection of Privacy Act* in 1993 launched a new, and still evolving, culture of privacy protection within the public service. As we have seen in this case, the protection of privacy is occasionally compromised, but the changed government culture palpably influences the behavior of public servants every day as they handle personal information. An unintended consequence of the changed culture is that people within government may be wary of sharing information with other public servants who require it in order to perform a legitimate work task. People in other ministries, or even in other branches within one ministry, are sometimes treated as if they are strangers outside of government, whose request for information is suspect.

A curious revelation in this case was that the person who supervises the MCFD ministry information security official knew little about the work done by that staff member. Due to the nature of the security official's work, and the information to which the position was privy, the supervisor felt they were not entitled to inquire about the work being performed. In most cases, the impact of the privacy culture is more subtle, and difficult to document, but this review believes it did constrain a number of interactions between people in different ministries, and even people within the same ministry, which in turn impacted human resource decisions.

The Office of the GCIO, Ministry of Citizens' Services, is working with other ministries to identify common and integrated programs, and support the practices, protocols and training which will facilitate the timely and lawful exchange of pertinent information. This initiative will help build an appropriate balance between the protection of personal information and the effective sharing of information to achieve good management and public policy objectives.

RECOMMENDATIONS

- 1. The BC Public Service Criminal Records Check Policy should be reviewed, in consultation with the Government Chief Information Officer, with an eye to expanding the types of positions which are considered for designation as subject to a criminal records check. In particular, positions which provide access to personal information systems should be considered.**

Historically, government's first priority was to prevent children from being exploited or harmed by people in positions of trust. The 1996 *Criminal Records Review Act* provided a strong system for checking the criminal records of persons who apply to work with children.

Based on the Public Service Criminal Records Check Policy, other positions also required checks, notably those in the law enforcement and some other fields where a high level of trust was critical. A more comprehensive policy, for positions not working with children, was introduced in March 2009. The new Criminal Records Check Policy (see appendix D) represented an important improvement over previous policy, both with respect to the procedure for conducting checks, and the range of positions which should be considered for designation as subject to a check. The criteria for designating positions was expanded from law enforcement and working with people in government care, to law enforcement, working with vulnerable adults, custody or control of significant government assets, and custody or control of information systems. The term "custody or control" of information systems suggests a higher level of authority than simple access to a system.

Although it appears that personal information was not used for criminal purposes, this case raises awareness of the potential vulnerability of personal information in the custody of government. Criminal record checks are not a guarantee that personal information can never be used this way. However, screening for persons with a criminal record which is relevant to the job they will be performing, does reduce risk. A person with a record for impaired driving may not represent a risk to the security of personal information. A person with a record for theft and fraudulent activity certainly does. The policy should ensure that the requirement for a criminal record check contemplates the job duties of an employee, and the type of information that may be accessible to them in the course of their work.

This recommendation concerns the balance struck between the privacy interests of government job applicants, and the privacy interests of citizens who have entrusted their personal information to the government. A broader range of government positions requiring a criminal record check would unquestionably shift this balance toward citizens.

- 2. In the longer term, as technology advances, the BC Public Service Agency and the Ministry of Public Safety and Solicitor General, should explore ways to enhance the thoroughness and integrity of background checks.**

There are a number of opportunities to improve existing criminal records checks procedures. Fingerprinting provides reliable identity verification, but it is cumbersome, costly and time consuming. As new digital technologies and other innovations become available, government should ensure it is employing the best techniques to obtain an accurate and complete picture of an applicant's criminal history, if one exists. This may also involve expanding the use of alternative employment and background checks that go beyond ascertaining the existence of a criminal record (the Ministry of Public Safety and Solicitor General is named in this recommendation because it is currently responsible for administering the government's criminal record check program).

- 3. A new human resource policy should be introduced to complement the current Criminal Records Check Policy. This new policy would mandate the steps to be taken when a government employee is arrested, charged, or convicted of a criminal offence.**

The recommended policy would, in the first instance, ensure that information about the event is communicated to a senior executive. That person would identify a lead investigator, who would maintain responsibility for the file. Not all allegations or convictions are relevant to the employee's work, and a lead investigator could make an early determination about whether the arrest, charge or conviction has a workplace impact. If it does, policy would provide for continued leadership, and communication between the program area manager, the police, and specialized labour relations advisors in the BCPSA. The existing Human Resource Transformation project, earlier endorsed by the Deputy Ministers Council, will assist the BCPSA in providing timely access to specialist expertise.

- 4. The Ministry of Children and Family Development and the BC Public Service Agency should confirm the transition plan for human resource services, to ensure clarity in the respective roles and responsibilities of Strategic Human Resources and the BC Public Service Agency.**

As MCFD began the devolution of transactional human resource functions to the BCPSA, participants believed they shared an understanding of when and how functions would be transferred to the BCPSA. The evidence of this case, and the interviews with Strategic HR and BCPSA staff, suggest there is continued confusion around the roles and accountabilities of each organization. The BCPSA and MCFD Executive should meet and ensure a common understanding about the required transition.

- 5. Following a review of this report, and the companion report on the privacy breach, the Ministry of Children and Family Development should review the judgement exercised by the managers involved and identify remedial action to ensure managers have the direction, training and support to respond more effectively to complex issues.**

Ministry of Housing and Social Development officials acknowledge that they should have linked sooner with the relevant managers in MCFD concerning the status of their investigation. However, the majority of missed opportunities, information dead-ends, and unconfirmed assumptions can be attributed to communication breakdowns in MCFD. This large and complex ministry has experienced many changes in recent years. The lessons of this case provide material for consideration by the ministry executive. Among other issues, there is a need to ensure that managers and supervisors have the requisite skills and knowledge before they embark on investigative or disciplinary tasks. Training in labour relations is readily accessible, and a new Corporate Learning Centre, part of government's Human Resource Transformation project, will assist in providing consistent training across government.

- 6. The Deputy Ministers' Council should review how external investigative agencies link with government when public servants are the subject of a criminal investigation. The aim of the review would be to ensure that the right information gets to the right people in government in a timely manner, while simplifying the process for police and other enforcement agencies.**

The Government Security Office (GSO) of the Ministry of Finance played a role in the early stages of this matter and staff from four ministries eventually had contact with the RCMP. This case presents an opportunity for government to take a fresh look at inter-ministerial coordination of information arising from external investigations. The role of the GSO is not well known within government and it would be timely, in the course of the proposed review, to examine the office's scope, mandate and relationship to other ministries.

APPENDIX A

Human Resource Review Involving the Ministry of Children and Family Development, Ministry of Housing and Social Development and the BC Public Service Agency

TERMS OF REFERENCE

Intent

This is an investigation of the human resource issues related to a privacy breach involving an employee of the Ministry of Children and Family Development. The purpose of this review is to examine the decisions and actions undertaken by the employees involved, the context in which those decisions were made and the supporting policies and practices that were applied. The information gathered from this review will be used to take appropriate remedial action to improve HR policies, practices and training and to ensure the environment in which our HR professionals work enables appropriate and timely action and decision making.

Background & Context

In April 2009, during the course of an unrelated investigation, the RCMP seized documents containing sensitive personal information related to the clients of the ministries of Housing and Social Development and Children and Family Development. An investigation is being undertaken of human resource actions with regard to this matter.

Objectives

The objectives of this investigation are to:

- Identify the various parties that were involved in the human resource processes and decisions;
- Confirm the events and facts pertaining and relevant to the human resource processes;
- Assess the human resource policies, practices and judgment applied by those individuals;
- Identify where improvement is required in existing policies, the application of those policies or in the operating principles and practices of HR and Management staff in managing these types of matters.

Scope

The following areas are within the scope of this review:

- The circumstances surrounding the handling of the employees involved; what decisions were made, who made them and what were the outcomes of those decisions.
- Government's human resource processes, policies, training and practices.

Out of Scope

- Government's processes, policies, system, training and practices associated with privacy matters.
- The circumstances of the privacy breach, how it was managed and steps taken to remediate the situations associated with the client files.

Deliverables

The report will include:

- A review of the decisions and actions taken.
- Identification and review of relevant human resource management policies, processes and practices in place at the Public Service Agency, MCFD and HSD and whether they were adhered to in this case.
- Proposal for short term actions and long term remedial approaches to address any inappropriate decisions, actions, practices or policies identified.

Approach

The review will be conducted by Bert Phipps, an Assistant Deputy Minister with the Corrections Branch, Ministry of Public Safety and Solicitor General. To ensure objectivity, the Head of the BC Public Service Agency selected an individual that is not currently employed by any of the three ministries involved.

The final approach to the review will be agreed to by Mr. Phipps and the Head of the BC Public Service Agency, but is anticipated to include the following:

- gathering and reviewing documentary evidence including all materials gathered to date,
- survey of relevant legislation, policies, practices, systems protocol,
- conducting interviews of or meetings with involved parties and government officials,
- reviewing and discussing relevant findings with the Head of the BC Public Service Agency.

A final report will be submitted to the Head of the Public Service Agency no later than January 29, 2010.

APPENDIX B

PERSONS INTERVIEWED FOR THIS REVIEW

1. Sergeant, Commercial Crime Section, Royal Canadian Mounted Police
2. Corporal, Commercial Crime Section, Royal Canadian Mounted Police
3. Investigator, Special Investigation Unit, Insurance Corporation of British Columbia
4. Director, Risk Mitigation, Security and Business Continuity, Government Security Office, Risk Management Branch, Ministry of Finance
5. Risk Mitigation Consultant, Government Security Office, Risk Management Branch, Ministry of Finance
6. Chief Human Resource Officer, Interior Health Authority
7. Manager, Medical Benefits Program, Provincial Child and Youth with Special Needs Operations, Provincial Services Division, Ministry of Children and Family Development
8. Senior Director, Provincial Child and Youth with Special Needs Operations, Provincial Services Division, Ministry of Children and Family Development
9. Senior Executive Director, Provincial Services Division, Ministry of Children and Family Development
10. Executive Director, Youth Custody Services, Provincial Services Division, Ministry of Children and Family Development (Acting Assistant Deputy Minister, August 2009)
11. Strategic Human Resource Planner, Strategic Human Resources, Ministry of Children and Family Development
12. Strategic Human Relations Planner, Strategic Human Resources, Ministry of Children and Family Development
13. Director, Sectoral Relations, Strategic Human Resources, Ministry of Children and Family Development
14. Senior Executive Director, Strategic Human Resources, Ministry of Children and Family Development
15. Ministry Information Security Officer, Corporate Management Branch, Ministry of Children and Family Development

16. Director, Information Management and Governance, Corporate Management Branch, Ministry of Children and Family Development
17. Ministry Chief Information Officer, Corporate Management Branch, Ministry of Children and Family Development
18. Ministry Investigator, Prevention and Loss Management Services, Regional Services Division, Ministry of Housing and Social Development
19. Regional Operations Director, Prevention and Loss Management Services, Regional Services Division, Ministry of Housing and Social Development
20. Assistant Deputy Minister, Regional Services Division, Ministry of Housing and Social Development
21. Executive Director, Strategic Human Resources, Ministry of Housing and Social Development
22. Senior Advisor, Information Access Operations, Ministry of Citizens' Services
23. Information Privacy Analyst, Information Access Operations, Ministry of Citizens' Services
24. Senior Security Analyst, Shared Services BC, Ministry of Citizens' Services
25. Human Resource Consultant, BC Public Service Agency
26. Labour Relations Specialist, BC Public Service Agency
27. Director, Labour Relations and Advocacy, Vancouver Island Region, BC Public Service Agency
28. Regional Director, Client Services, Vancouver Island Region, BC Public Service Agency
29. Regional Director, Client Services, Southern Interior Region, BC Public Service Agency
30. Executive Director, Risk Management Branch, Ministry of Finance

APPENDIX C

How criminal records checks are applied to government employees

There are two systems within government which work to prevent people from getting jobs where their criminal record would represent a risk to the public, government staff or government assets and systems. The *Criminal Records Review Act* authorizes checking for criminal records for people who work with children, in the public service, in schools, care facilities and non-profit organizations. This requires criminal records checks at the time of employment, and every five years thereafter. While the employee must consent to the check, the information provided by the RCMP is delivered directly to the government.

The Public Service Criminal Record Check Policy applies to a number of government employees who do not work with children. The policy requires checks for all executive positions (deputy ministers, associate deputy ministers and assistant deputy ministers). It also recommends that four other types of positions be considered for designation: positions which work with vulnerable adults, positions involving law enforcement, and positions with custody or control of significant government assets, and custody or control of information management systems. Consents for record checks were formerly submitted to police by job applicants themselves. The police results were then returned to the job applicant, who would pass them on to the public service. Policy changes in March 2009 require that the results of the criminal record check are provided directly by the RCMP to the government.

Criminal records checks under both the *Criminal Records Review Act* and the Criminal Record Check Policy are administered by the Ministry of Public Safety and Solicitor General.

These two procedures generally rely on “name checks”. The employee provides picture identification and the name found on the identification is checked against the Canadian Police Information Centre (CPIC) database. If there is any uncertainty about the employee’s identity, a check against fingerprints can be conducted (law enforcement positions require fingerprint checks in every case).

APPENDIX D

PUBLIC SERVICE CRIMINAL RECORD CHECK POLICY

14. Criminal Record Check Policy (Human Resources Policies)

This policy covers the requirement for criminal record checks for designated positions within the BC Public Service. The directive supports the Core Policy of ensuring that “government is supported by a professional public service that has the knowledge, skills, and abilities to achieve current and future objectives.”

This policy covers criminal record checks other than those required under the Criminal Records Review Act. This policy applies to new employees and employees changing positions only.

A criminal record check may form part of the process of assessing an applicant’s relative suitability for a designated position. The Canadian Charter of Rights and Freedoms, the Human Rights Code, and Supreme Court of Canada decisions impose strict limits on how the employer uses the information from these records. A criminal record check must relate to the requirements of the position.

A criminal record check is a search for convictions, penalties and outstanding charges as required under this policy.

All applicants for designated positions within the public service must successfully complete a criminal record check before their appointment is confirmed.

A deputy minister, including the deputy attorney general and deputy solicitor general, may require additional enhanced security screening checks for some applicants in particularly sensitive positions. These additional checks are outside the scope of this policy.

Purpose of Criminal Record Checks

The purpose of criminal record checks is to:

- Protect the safety and security of vulnerable people in the care of public service employees
- Maintain the security and integrity of provincial law enforcement
- Protect significant financial and information assets of the province
- Maintain the public trust and confidence in public service employees

Designated Positions

A director, on the recommendation of the hiring manager, will designate positions requiring criminal records checks. The deputy minister must approve all designated positions. Positions with the following primary functions may be designated:

- Care, custody, counseling, or legal responsibility for vulnerable adults (see definition of vulnerable adult below) who are clients of the government or are under government care.
- Law enforcement, where duties involve enforcement, investigations, inspections, the control, care and custody of people and/or property, access to sensitive enforcement or investigations information, the administration of the justice system and the prosecution service.
- Responsibility for the custody and control of significant government assets and information management systems, technology and security.
- Interfacing with third-party and/or alternate service delivery organizations where the third party requires a criminal record check.

Positions with the following functions must be designated:

- Senior executive positions (assistant deputy minister, associate deputy minister, deputy minister, or equivalent) including those who change positions.

Definition of Vulnerable Adults

For the purposes of this directive, vulnerable adults are those 19 years or older, who:

- Because of a physical or mental disability, do not have the capacity to cope with or remove themselves from a threatening or abusive situation (physical or mental incapacity may be indicated in formal documentation or by the treatment required)
- Have limited capacity because of illness, medication, treatment, or substance abuse
- Have little or no choice with respect to their situation and are unable to voluntarily assume or manage risks associated with the accommodation provided, the programs they are enrolled in, or the care that they are receiving
- Because of a custodial arrangement, do not have the right and opportunity to remove themselves from a threatening or abusive situation

Administration

Applicants must consent to criminal records checks before they are conducted. If applicants do not give their consent, their appointment cannot be confirmed.

Care must be taken to balance the rights of applicants to personal privacy and freedom from discrimination with the government's responsibility to protect the public, employees, and assets. The results of criminal record checks will be held in strictest confidence. Records must be stored in a secure manner and records for applicants who are not hired must be destroyed. Criminal record checks should be re-administered every five years from the date of hire unless the risks associated with the position make less frequent checks more appropriate. The requirement for a recheck must be included in the offer of employment letter and is a condition of employment. If the employee refuses to consent to a recheck they can be terminated.

Deputy ministers are responsible for the final decisions where an applicant requests either a review of the designation of a position or a review of the hiring manager's decision to not appoint an applicant because of his or her record.

Hiring Practice

The BC Public Service recommends best practices in the [Hiring and Deployment Policy Statement](#). This process of evaluating the trustworthiness and reliability of applicants could also include checks of Provincial records, where the Province maintains information systems related to its own compliance or enforcement activities.

All of the Information gathered during the hiring process will be considered in the adjudication of criminal record check results. This information provides verification of the accuracy of the information the applicant has provided on their background, their reliability and past work performance.

Compliance with Criminal Records Review Act Requirements

The Criminal Records Review Act (CRRA) requires a criminal record check for every employee who works with children under the age of 19 years. If a position is designated in accordance with this policy and is also subject to the CRRA, and if risk identified for the position relates only to the safety of the children, organizations may choose not to require an additional criminal record check under this policy provided one has been completed under the CRRA.

Exceptions

Except in the case of statutory requirements under the CRRA, the director, on recommendation of the hiring manager may decide that the need for a record check may be negated when there are other adequate controls and procedures in place to mitigate risk. This decision and its rationale must be documented on the hiring file.

Where an organization can demonstrate that it will exceed the objectives set out in this policy, it will not be obliged to apply the specific record check procedures as set out in this policy.