Office of the
Information & Privacy
Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

INVESTIGATION REPORT F16-03

Mobile Device Management in B.C. Government

Drew McArthur
Acting Information and Privacy Commissioner for B.C.

October 18, 2016

CanLII Cite: 2016 BCIPC 50
Quicklaw Cite: [2016] B.C.I.P.C.D. No. 50

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

Look around and you will see people using smartphones everywhere, all the time. It may be stating the obvious, but mobile device use is increasing at a record pace.

Today, many of us are issued a mobile device by our employer. This makes sense in the modern business environment, as work can be performed from remote locations and at any hour, saving travel and facilitating logistics. Despite these convenience factors, mobile device use can be challenging for organizations. Precautions must be taken to ensure that the privacy and security of personal information is not compromised.

Given the widespread adoption of employer-issued mobile devices in the B.C. government, my office decided to assess the maturity level of government's approach to managing these devices.

I would like to acknowledge that this report was undertaken concurrently with an audit conducted by the Office of the Auditor General of British Columbia. My predecessor Elizabeth Denham and the current Auditor General, Carol Bellringer, determined that our offices should look for opportunities to cooperate. This would allow us to draw on one another's expertise and reduce potential overlaps when auditing or investigating the government. In this particular endeavour, the Auditor General focused on the security aspects of the government's use of mobile devices, while my Office focused on the privacy considerations.

This investigation was conducted at a specific point-in-time, from June to November 2015. Our two teams met with government representatives to collect information and documents, and then each office applied their own process to evaluate the materials.

Our investigators found that while policies were in place, they were often overlapping, inconsistent, and confusing. I am recommending that government take the opportunity to review and revise their policies regarding the use of mobile devices to be clear, concise and comprehensive. This will make them easy to understand and more importantly, easy to follow.

Rules need to be established and government employees must be trained on how to use portable tools while protecting information that might be accessed or stored on their mobile devices. Furthermore, where technical controls cannot be implemented, then education must be provided to ensure employees do not inadvertently compromise personal information.

Since this investigation, government has made a number of positive changes, including the introduction of their *Privacy Management and Accountability Policy*. Some of my concerns in the initial findings have been addressed by government as a result of the introduction of this policy and I find that encouraging.

My predecessor indicated in an earlier report that if the government treated the personal information in its possession the same way it treated money, then the information would be much more secure. I want to build on this idea by introducing the phrase “treat your cache like cash.” That is, treat the information in your data caches like cash. The loss of personal information is more expensive than the loss of money and can have many unforeseen consequences for individuals over time.

Finally, getting it right in the first instance is not the end of the journey. Policies, programs, guidelines, and training need to be continuously evaluated to ensure that our information remains secure in light of changing technology and the new capabilities of portable devices.

Drew McArthur
Acting Information and Privacy Commissioner
for British Columbia

EXECUTIVE SUMMARY

This investigation report from the Office of the Information and Privacy Commissioner ("OIPC") examines the management of mobile devices issued to employees by the B.C. government. It focuses on smart phones, tablet computers, and other devices that use mobile specific operating systems, and examines whether the management of personal information on those devices meets government's responsibilities under the *Freedom of Information and Protection of Privacy Act* ("FIPPA").

The OIPC assessed government's management of mobile devices based on three criteria: whether government has an appropriate privacy management program, whether the storage and retention of personal information accessed on mobile devices occurs only in Canada, and whether government has adopted reasonable security measures to protect that information.

Privacy management programs are the best way for public bodies to demonstrate compliance with their responsibility to protect personal information. During this investigation, government did not have an overarching privacy management program. OIPC investigators therefore sought to determine whether the elements of such a program were in place to adequately protect personal information accessed or stored on mobile devices. These elements are detailed in a 2013 guidance document, *Accountable Privacy Management in B.C.'s Public Sector*, and are organized around the need for a commitment to privacy compliance, adequate program controls, and ongoing assessment and revision.

The investigation determined that senior management in the ministries we examined did not demonstrate sufficient commitment to privacy compliance in the use of mobile devices by ministry employees. OIPC investigators found evidence that employees responsible for privacy management lacked the authority and resources necessary to implement and monitor program controls for privacy and mobile devices.

In several areas, we found a lack of those program controls that are integral to a privacy management program. The selected ministries did not maintain an inventory of personal information stored on mobile devices nor did they categorize the sensitivity of personal information in their custody. The investigation also found a large number of overlapping policies related to mobile devices that were difficult for employees to access and to understand. Employees were required to complete privacy training, but this training did not specifically relate to mobile devices and was not conducted frequently enough to ensure that employees were aware of their specific responsibilities. OIPC investigators also found that risk assessments were insufficient and that when

privacy breaches occurred, government’s breach and incident protocols were not consistently followed.

In addition, the investigation found a lack of agreement between the OCIO and the ministries regarding their roles and responsibilities for privacy management. A government-wide and ministry-administered approach to privacy management is useful for implementing overarching standards while accommodating specific ministry needs, but the respective responsibilities must be understood by each party.

In most cases, personal information on mobile devices will be stored on the device or on government servers. FIPPA and government policy restricts employees from storing personal information on applications that store data outside of Canada, but this investigation found that government does not have the technical capability to detect and prevent the use of those applications.

Government is required by FIPPA to make reasonable security arrangements to protect personal information on mobile devices. Based on the findings in the report by the Auditor General, and on my determination that key elements of a privacy management program were not present, I found that government is not meeting its statutory obligation to protect personal information stored on mobile devices.

After the start of this investigation, the B.C. government introduced a Privacy Management and Accountability Policy (“PMAP”). The PMAP includes the elements of a privacy management program and clearly assigns roles and responsibilities for its operation. This is a significant step forward in the management and protection of British Columbians’ personal information and the OIPC will follow up on its implementation.

1.0 INTRODUCTION, PURPOSE, AND PROCESS

1.1 INTRODUCTION

Today, many B.C. government employees are issued devices with mobile operating systems to perform their jobs. While mobile phones, tablets, and other devices help governments keep pace with an ever-changing work environment, they also pose unique implications for the privacy and security of the information collected, stored and accessed on them. This data can include the sensitive personal information of B.C. residents.

There are many noted security vulnerabilities associated with mobile devices. They can be easily stolen or lost, their communications may be intercepted and their security settings are often poorly configured by users. These challenges are further complicated by the variety of devices on the market and a growing demand by employees to use personal mobile devices for their employment activities.

Given the widespread use of mobile devices by government and the unique challenges they pose to privacy and security, former Commissioner Elizabeth Denham decided to examine how the B.C. government manages these devices in the context of compliance with FIPPA.

This investigation was conducted in coordination with an audit by the Office of the Auditor General of British Columbia ("Auditor General"), given our offices' joint interests in this topic. Each office has published a separate report in fulfilment of its respective statutory obligations and requirements.

The Auditor General focused on the security aspects of managing mobile devices whereas my Office focused on the privacy considerations. The scope of this investigation was limited to devices that use mobile operating systems, such as smartphones and tablets in use by employees in selected government ministries.

As the Acting Information and Privacy Commissioner for B.C., I have a statutory mandate to monitor a public body's compliance with FIPPA. This investigation was conducted in accordance with my powers under section 42(1)(a) of FIPPA.

1.2 OBJECTIVE, SCOPE, AND INVESTIGATION PROCESS

The mobile devices examined in this investigation are used to collect, access, and store personal information for government purposes. These include smartphones, tablet computers, and other devices that use mobile-specific operating systems (*e.g.,* Android, Apple iOS, or Blackberry operating systems).

The objective of this investigation was to assess whether government ministries manage the use of these mobile devices for government purposes in a manner that protects the privacy of personal information collected from employees and citizens. Specifically my investigators assessed:

- whether government has an appropriate privacy management program in place including privacy and security policies, training, privacy impact assessments, and security threat risk assessments;

- whether storage and retention of personal information occurs only in Canada as required by s. 30.1 of FIPPA; and

- whether personal information stored on government mobile devices is protected against such risks as unauthorized access, collection, use, disclosure, or disposal by reasonable security arrangements as required by s. 30 of FIPPA.

Five government ministries were selected for this investigation based on several factors including the number of reported security incidents and the sensitivity of data stored or accessed through mobile devices. These ministries were the Ministry of Children and Family Development (“MCFD”), Ministry of Finance (“MoF”), Ministry of Forests, Lands and Natural Resource Operations (“FLNRO”), Ministry of Justice (“MoJ”), and Ministry of Health (“MoH”).

Since this assessment was conducted government has made several significant changes that are relevant to my findings and recommendations. In December 2015 responsibility for government’s compliance with FIPPA was moved from the OCIO to the newly formed Privacy, Compliance and Training Branch (“PCTB”) of the Ministry of Finance. The Office of the Chief Information Officer (“OCIO”) remains responsible for setting policy and standards for telecommunications, information technology, and security. Therefore, the privacy responsibilities of the OCIO that are referred to in this report are now the responsibility of the PCTB.

In addition, since this assessment was conducted government has implemented the PMAP.[1] This policy likely addresses some of the findings and recommendations issued in this report, however, as it was not in place at the time of this assessment, I have not considered its implications for the management of mobile devices.

[1] Privacy Management & Accountability Policy, Government of British Columbia, available at: http://www2.gov.bc.ca/gov/content/governments/services-for-government/policies-procedures/privacy-policy.

1.3 INVESTIGATION PROCESS

My predecessor announced her intention to investigate this matter by way of a letter to the OCIO on June 17, 2015. She requested the OCIO's assistance in disseminating information about this investigation to the selected ministries and also requested a list of key staff responsible for the management of mobile devices in each ministry.

The OIPC undertook this investigation in conjunction with an audit conducted by the Auditor General. Our offices coordinated a survey of the selected ministries and conducted interviews of employees at those ministries. While the OIPC has jurisdiction to investigate matters of information security as well as the protection of privacy, for the purposes of this investigation this Office focused primarily on the privacy implications associated with government's management of mobile devices.

Investigators with the OIPC took the following steps to meet the objectives of this investigation:

- Reviewed risk assessments and policies and procedures of the OCIO and selected government ministries;

- Assessed the adequacy of these policies and procedures and the extent of compliance with these policies and procedures; and

- Where appropriate, made recommendations to strengthen policies or practices.

The assessment criteria were based on requirements under FIPPA and guidance material from the OIPC document *Accountable Privacy Management in B.C.'s Public Sector*.[2] The investigation was conducted from June through November 2015 and included interviews with chief information officers (CIOs) and additional staff responsible for management of mobile devices in the OCIO and each of the selected ministries.

OIPC investigators requested and analyzed more than 200 documents including government's mobile device strategy, privacy and security policies and guidelines, risk assessments, training materials, and inventories of mobile device purchase and use.

I provided the OCIO and each of the ministries with a copy of these observations and requested their feedback regarding any factual inaccuracies, omissions or

[2] https://www.oipc.bc.ca/guidance-documents/1545.

misinterpretations. I received written feedback from two ministries, MoH and MoF, as well as from the OCIO divisions responsible for privacy and security. Their feedback was considered in the drafting of this report.

1.4 APPLICATION OF FIPPA

Public bodies can best demonstrate compliance with FIPPA's requirements to protect personal information by implementing a privacy management program. This is outlined in OIPC's 2013 guidance document entitled *Accountable Privacy Management in B.C.'s Public Sector*. The program can be tailored to the unique needs of each public body. This report reviews whether the OCIO and the five ministries selected had a privacy management program (or at least some elements of one) and whether it was adequately applied to mobile devices. FIPPA also contains provisions that address storage of and access to personal information in the custody or under the control of public bodies. Subject to some exceptions, s. 30.1 of FIPPA states that "a public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada." This section of FIPPA is particularly relevant to this investigation because many mobile applications store personal information outside Canada or access personal information on the device from outside Canada.

Section 30 of FIPPA imposes a statutory obligation on public bodies to protect personal information in their custody or control by "making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure and disposal." The nature and level of security arrangements depends on the sensitivity of the information to be protected and the medium through which the information is collected, accessed, stored and disclosed.

2.0 OVERVIEW OF MOBILE DEVICE MANAGEMENT IN B.C. GOVERNMENT

2.1 POLICIES AND PROCEDURES

In May 2006, the provincial Cabinet mandated that the OCIO set standards and generally oversee and approve the province's information and communications technology.[3] Mobile devices are a key component of that technology. The

[3] Ministry of Technology, Innovation and Citizens' Services; Office of the Chief Information Officer; Governance. www.cio.gov.bc.ca/cio/about/governance/governance.page

province's *Core Policy and Procedures Manual*[4] outlines the respective privacy and security responsibilities of the OCIO and ministry CIOs.

Chapter 12 of the *Core Policy and Procedures Manual* defines the authorities, responsibilities, and accountabilities for information and technology management. It explains the roles and responsibilities for Information Management and Information Technology ("IM/IT") resources in government and describes the OCIO as the central authority responsible for developing and maintaining IM/IT policies, procedures, and standards across all ministries. The *Information Security Policy* (ISP) is one of the four major policy manuals that support this chapter of the *Core Policy and Procedures Manual*.

The ISP was adopted by government in 2006 and is based on an International Organization for Standardization ("ISO") standard for information security.[5] This standard provides a structured approach to identifying information security activities and improving information security management within an organization. Version 2.2 of the ISP (updated in 2012) was the version in place at the time of this investigation and was the focus of my Office's review.

2.2 ROLES AND RESPONSIBILITIES

The *Core Policy and Procedures Manual* states that, as the central authority for the government of B.C., the OCIO is mandated to:

- set policies, procedures and standards governing citizens' information held by the Province, and ensure that staff and contractors are aware of their rights, roles and accountabilities for the security, privacy and management of government's IM/IT assets;

- provide the overall strategic direction and policy for securing government's information technology and government records including electronic information, and ensure that measures are established to assess compliance with IM/IT security policies, procedures and standards; and

- develop mechanisms and processes to ensure compliance with IM/IT policies, procedures and standards, and inform ministry CIOs of their responsibilities in complying with IM/IT policies, procedures and standards.

[4] http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm
[5] ISO 27002:2005.

While the OCIO sets the general policies and standards, the *Core Policy and Procedures Manual* states that each ministry CIO is accountable for ensuring the privacy and security of IM/IT assets under their jurisdiction for their ministry.[6] This includes adequately protecting all personal information holdings in physical, electronic and digital formats by implementing security measures proportionate to the value and sensitivity of that information.

In practice, however, the OCIO has taken on roles and responsibilities that are assigned to ministries by policy. The OCIO, for example, exercises specific functions related to mobile device management, including:

- conducting security risk assessments on mobile devices and operating systems;
- investigating information incidents;
- managing privacy breaches; and
- maintaining a list of employees who can access government Exchange servers[7] through their mobile devices.

Privacy and security staff within each ministry are then expected to implement additional safeguards that may be needed based on their unique information holdings and the level of risk associated with personal information.

2.3 TECHNICAL CONTROLS

Government uses a mobile device management tool to manage devices that are authorized to access personal information contained on government servers. The tool is centrally controlled by the OCIO and ministries must make a request to connect devices to the government network. Requests are received by the OCIO and an account is set up for the employee using the mobile device.

Once an account is established, the employee can connect multiple mobile devices using the same account. After they connect, the devices can be expected to receive baseline security settings from the server. These settings (discussed in more detail in the Auditor General’s report[8]) include encryption of the device's storage, setting the period of inactivity before the screen locks, and configuring anti-malware software.

[6] Role of the Ministry Chief Information Officer (MCIO). www.cio.gov.bc.ca/cio/about/governance/role_cio/ministry_cio.page.

[7] Exchange servers contain email, calendar, and contact information.

[8] Office of the Auditor General of B.C. - Management of mobile devices: Assessing the moving target in B.C. – October 2016.

3.0 OBSERVATIONS AND FINDINGS

My observations and findings are divided into three subsections corresponding to the objectives for this investigation:

1. Adequacy of the Privacy Management Program
2. Storage and Access Outside Canada
3. Reasonable Security Arrangements

Each of the subsections below include my expectations for compliance with legislative requirements in FIPPA, specific examples that illustrate areas of concern, and my findings and recommendations based on the results of this investigation.

3.1 ADEQUACY OF THE PRIVACY MANAGEMENT PROGRAM

The best way for a public body to demonstrate compliance with their obligations to protect personal information under FIPPA is to implement a privacy management program. This has been emphasized in numerous investigations conducted by this Office.[9]

The first objective of this investigation was to determine whether government as a whole, or the five specific ministries examined, had such a program in place. OIPC investigators requested information and documentation that demonstrated the presence of a privacy management program and the proper application of its principal elements to the management of mobile devices.

The principal elements of a privacy management program should include:

- adequate resources for the development, implementation, and monitoring of privacy controls;
- the presence of applicable policies and procedures;
- up-to-date documentation of risk assessment and mitigation strategies;

[9] Office of the Information and Privacy Commissioner Investigation Reports F16-01 (www.oipc.bc.ca/investigation-reports/1907); F15-01 (www.oipc.bc.ca/investigation-reports/1775); and F13-02 (www.oipc.bc.ca/investigation-reports/1546).

- adequate training delivered regularly;
- adequate information incident management processes;
- compliance monitoring; and
- regular reporting to the executive.

During the timeframe of this investigation, government did not have an overarching privacy management program in place, nor did it have one specifically related to mobile devices.

In response to our early feedback, the OCIO acknowledged the need for a privacy management program to mitigate privacy and security risks. Shortly after my investigators' initial inquiries, the government established and implemented the PMAP to address this significant deficiency. The adequacy of the PMAP is outside the scope of this investigation; however, I intend to follow-up on its implementation.

Though government lacked an overall program to protect personal information, OIPC investigators nonetheless examined whether any of the elements of a privacy management program were present and if so, whether they were adequately applied.

The following sections detail the results of that examination and are based on the elements documented in the 2013 guidance document, *Accountable Privacy Management in B.C.'s Public Sector.*

Demonstrating Senior Management Commitment and Support

Senior management commitment to a privacy-protective culture is key to an effective privacy management program compliant with legislative requirements and privacy best practices. In the public sector, senior management support can be demonstrated by:

- creating and fostering a culture of privacy awareness;
- designating an individual responsible for the public body's privacy compliance and practices;
- ensuring that all resources necessary to develop, implement, monitor, and adapt a privacy management program are available to the individual responsible for the public body's privacy compliance and practices; and

- implementing reporting mechanisms to ensure that senior management are informed, on a regular basis, whether or not the program is functioning as expected.

Areas of Concern

OIPC investigators found several important areas where support of senior management was either lacking or could be improved. They observed that staffing resources were not always adequate: for example, the CIO and staff responsible for privacy for FLNRO were also responsible for the privacy management of five other ministries.[10]

I do not believe this staffing arrangement is adequate. Given the extensive responsibilities associated with privacy and security management in each ministry, I would expect that each would have its own privacy officer responsible for a privacy management program. Ministry staff also told my investigators that staffing resources could improve.

OIPC investigators also observed inadequate resources dedicated to compliance monitoring. With the exception of MoH, the responsibility to conduct an internal audit program was not assigned to any staff in the ministries examined. While MoH did have an internal audit program in place, it did not address the use of mobile devices.

In general, it was evident to my investigators that senior management did not take sufficient steps to address the unique risks associated with the use of mobile devices and the need, for example, to deploy automated tools to enforce controls and monitor compliance with policies.

I find that senior management in the selected ministries did not ensure appropriate resources were available to mitigate the specific risks associated with mobile devices, and therefore did not demonstrate sufficient commitment to a privacy-protective culture to ensure compliance with FIPPA and consistency with privacy best practices.

Designate and Empower a Privacy Officer

The head of a public body (or his or her delegate, *i.e.,* the privacy officer), is responsible for ensuring compliance with FIPPA generally and is accountable for designing and managing the privacy management program. The privacy officer establishes and implements program controls; conducts ongoing assessment

[10] Ministries in the natural resource sector core are: Environment; Forests, Lands and Natural Resource Operations (FLNRO); Energy and Mines; Natural Gas Development; Agriculture; and Aboriginal Relations and Reconciliation.

and revision of program controls; and monitors, audits, and documents the implementation of the privacy management program.

Areas of Concern

At the time of this investigation, each ministry had appointed individuals responsible for the privacy and security of mobile devices. However, these individuals did not have the authority and resources that I would expect to see of an empowered privacy officer.

For example, these individuals were not empowered to establish program controls or conduct ongoing assessments. These shortcomings were acknowledged in two internal ministry briefing documents provided to my investigators. Those documents, directed in one case at the OCIO and in another case at a ministry CIO, cited a lack of internal resources and expertise to adequately manage risks associated with mobile devices.

I find that, in the selected ministries, senior management did not adequately empower those responsible for privacy compliance.

RECOMMENDATION 1: Each government ministry should empower a privacy officer to develop, implement, monitor, and adjust the privacy management program. Ministries should ensure the privacy officer has adequate resources to meet privacy management responsibilities.

Compliance Reporting

The OIPC's 2013 guidance document *Accountable Privacy Management in B.C.'s Public Sector* states:

> A privacy management program's controls need to include several types of reporting mechanisms. The goal should be to ensure that the Privacy Officer and executive management are informed, on a regular basis, whether the program is functioning as expected, how and why it is not, and of the proposed fixes.[11]

It also states that internal audits of security safeguards should form a key component in a privacy management program.[12]

[11] Office of the Information and Privacy Commissioner. *Accountable Privacy Management in B.C.'s Public Sector*, p. 7. (https://www.oipc.bc.ca/guidance-documents/1545).

[12] Office of the Information and Privacy Commissioner. *Accountable Privacy Management in B.C.'s Public Sector*, p 6. (https://www.oipc.bc.ca/guidance-documents/1545).

The ISP tasks ministries with ensuring that security policies and processes are implemented and adhered to through periodic self-assessments and the initiation of independent assessments, reviews, or audits to assess compliance with policy.[13] In addition, ministries must develop a plan each year that identifies those information systems that will undergo a security review.[14]

The ISP also requires that ministries regularly test information system technical control compliance to:

- determine whether information system patches have been applied;
- confirm that system technical controls have been implemented and are functioning as designed; and
- perform technical compliance monitoring to verify that unauthorized connections or system changes have not been made.

Areas of Concern

Compliance Monitoring—According to the ISP, ministries must conduct an annual security review.[15]

However, OIPC investigators found no evidence that ministries conducted mobile device usage assessments, reviews, or audits with respect to privacy. Some of the ministries stated that they did not have the capacity, expertise, resources, or tools to perform such reviews, and they expressed the view that this function should be provided centrally by the OCIO.

This is particularly concerning given that OIPC investigators found instances where privacy and security policy requirements were not followed. For example, my investigators found evidence of many unauthorized devices connected to the government's mobile device management tool.[16] Some devices purchased by ministries were not authorized for use, and employees were connecting their personal devices to government servers, a practice not authorized by government.

Both the ministries and the OCIO were surprised by this finding when OIPC investigators brought it to their attention – even though the information was derived

[13] Office of the Chief Information Officer–Information Security Policy, October 2012–ISP 11.2.1 a.
[14] Office of the Chief Information Officer–Information Security Policy, October 2012– SP 11.2.1 b.
[15] Annual Information Security Review (an assessment provided by OCIO based on ISO 27002 international standard for information security).
[16] Office of the Chief Information Officer–Mobile Device Access Service Devices & OS Approval Status, last updated August 18, 2015.

from the OCIO's own report. The ministries stated that they were not aware that such reports were available and stated that these reports would help them monitor staff compliance. The OCIO told my investigators that ministries are only provided with reports from the mobile device management tool upon request.

This finding indicates a lack of coordination and understanding within government regarding privacy compliance and has resulted in confusion around roles and responsibilities for mobile device management.

Implementing Compliance Controls—OIPC investigators did not find any automated tools or processes in place to regularly test technical control compliance. Information about software updates and approved patches was communicated to staff through newsletters, email, and occasionally by phone, but it was left to device users to take action. There were no processes to determine whether software updates and patches had actually been applied as required.

While some of the OCIO's security requirements were enabled through the mobile device management tool, adoption of other security controls was largely left to the discretion of the end-user employee or the ministry business area. No mechanisms were in place to ensure that only authorized devices were allowed access to government data.

Privacy and Flexibility—The security staff at the OCIO stated that the lack of privacy and security controls and other best practices, such as central administration of controls and monitoring of employee compliance, is consistent with its *Device Strategy.*[17] This strategy prioritizes the usability of IT devices to ensure that employees can perform their duties without limitations. [18]

In this device strategy, the OCIO states:

> "[g]overnment IT organizations must continue to reinforce the culture of the trusted employee ensuring that this principle is at the forefront of IT design and service delivery. A culture that embraces this concept will make decisions, even small ones, that do not impact the abilities of trusted employees to perform their work. This is critical, as it is easy to justify simple decisions that remove or limit device usability/functionality under the guise of control, security, policy and management.[19]

I am concerned that transferring risk management from centralized IT departments to the individual employee fails to acknowledge that the majority of threats to privacy

[17] Office of the Chief Information Officer – "Device Strategy: Next Generation Device Services", March 2015.

[18] Office of the Chief Information Officer – "Device Strategy: Next Generation Device Services", March 2015; p. 12.

[19] See note 16.

and security of organizational data are posed by employees themselves, often accidentally. This model also ignores industry best practices and standards which recommend central enforcement of key security settings and automated monitoring and reporting on compliance with privacy and security controls.[20] Ministry information security officers told my investigators they were also concerned that this approach prevented the automatic implementation of privacy and security controls. **I find that government did not have an adequate audit program in place to determine compliance with privacy obligations under FIPPA.**

RECOMMENDATION 2: Ministries should monitor and audit compliance with privacy policies and adopt proactive solutions to detect unauthorized use and disclosure of ministry information.

RECOMMENDATION 3: Government should review its mobile device management strategy to ensure that employees are provided with adequate training and guidance to understand the privacy and security risks posed by mobile devices.

Where government policy places an unreasonable expectation on employee's technical knowledge, government should ensure the security of personal information is not compromised in favour of flexibility.

Personal Information Inventory

Accountable Privacy Management in B.C.'s Public Sector highlights the importance of creating a personal information inventory. It states:

> Creation and maintenance of a personal information inventory is a good example of why public bodies need to document their activities—accountability is at the core of FIPPA and adequate documentation is essential to achieving, and demonstrating, accountability for privacy protection.[21]

A public body cannot provide adequate security for personal information in its custody or control if it does not know where that personal information is collected and stored. The personal information inventory should catalogue the different

[20] NIST Cybersecurity Practice Guide – "Mobile Device Security", November 2015; "NIST Guidelines for Managing the Security of Mobile Devices in the Enterprise" June 2013; ISACA "Securing Mobile Devices", An ISACA Emerging Technology White Paper, August 2010.

[21] Office of the Information and Privacy Commissioner, *Accountable Privacy Management in B.C.'s Public Sector*, p. 8. (https://www.oipc.bc.ca/guidance-documents/1545).

types of data held (*e.g.,* employee data, client data, ministry-owned data, and data co-owned with another organization) and where the personal information is stored (*e.g.,* servers, mobile devices, desktops, in the cloud).

Areas of Concern

Lack of a Personal Information Inventory—This investigation found many instances where personal information such as email and contact information was downloaded from government servers and stored on mobile devices. However, ministries did not maintain an inventory of the types of personal information being stored on mobile devices.

When presented with these observations, the OCIO committed to working with the ministries to establish a personal information inventory.

I find that the ministries selected for this investigation did not maintain an accurate inventory of personal information stored on mobile devices and did not categorize the sensitivity of the personal information holdings.

RECOMMENDATION 4: Ministries should conduct a thorough review of all personal information currently stored on mobile devices and then create an inventory of the types of personal information that is commonly stored.

Compliance Policies

A public body must have policies and procedures for protecting personal information and they must inform employees about their roles and responsibilities in this regard.[22] Policies should be easy to locate and readily available to employees in an understandable and actionable format.

The OCIO provided a number of its policies that apply to mobile device management. These included the *Core Policy and Procedures Manual*, the ISP, the *Appropriate Use Policy*, the *Working Outside the Workplace* policy, and the *Information Incident Management Process*. While the ISP references mobile devices, the other policies provided general direction on information management and did not specifically focus on the unique characteristics of mobile devices. The OCIO did provide a guidance document related to the risks

[22] Office of the Information and Privacy Commissioner, *Accountable Privacy Management in B.C.'s Public Sector*, p. 11. (https://www.oipc.bc.ca/guidance-documents/1545).

of downloading applications onto mobile devices as well as a “policy summary guidance” document on mobile computing.

Each ministry also provided a set of guidance documents regarding the use of mobile devices by employees within that ministry. For example, social workers at MCFD were required to comply with policies for text messaging with clients and contractors and were provided with guidance on the use of contractor-owned devices.

Areas of Concern

Policy Confusion—Many of the general privacy and security policies provided to my investigators could be extended to include mobile devices, but their broad nature left employees uncertain as to their interpretation.

OIPC investigators also found some discrepancies between OCIO policy documents and ministry guidelines.

For example, the ISP did not permit the use of non-government devices for government purposes unless authorized.[23] MCFD guidelines for contractors allowed a contractor to use their own mobile devices to manage client information. [24] My investigators could not determine whether these guidelines were sufficient to authorize the use of personal mobile devices. When my investigators brought this to the attention of the OCIO, the OCIO believed MCFD’s actions contradicted policy and committed to follow up with the ministry.

Accessibility of Policies—I am also concerned there are too many policies and guidance documents that may apply to mobile device management. This makes it difficult for employees to access and understand them.

Ministry staff noted that the ISP was long, confusing, and hard to implement. Policies should be presented in a format that is understandable to an employee with limited technical expertise.

OIPC investigators also looked at the *Appropriate Use Policy*, a high-level document that provides an overview of requirements in other policy documents that employees must follow. Although the *Appropriate Use Policy* referred to the use of mobile devices, it did not reference security controls that employees must implement to ensure compliance with privacy requirements.

[23] Office of the Chief Information Officer–Information Security Policy, October 2012 – ISP 2.1.4 d.
[24] Ministry of Children and Family Development (MCFD) – “Contractor’s Information Management Guidelines” – November 2014; p. 3.

OIPC investigators found instances where multiple policies related to the same topic, and employees were required to comply with each policy. For example, there were several documents[25] that addressed downloading applications onto mobile devices, each referring the reader to additional and overlapping guidance documents. The resulting confusion was compounded by the fact that these policies were not all available in the same place.

I find that the general nature of the ISP and the Appropriate Use Policy confused employees about their application to mobile devices. The excessive number of other policies and guidance materials made it difficult for employees to access and understand them. Therefore these policies do not fulfill the objective of providing adequate privacy protection for personal information stored on mobile devices.

RECOMMENDATION 5: Compliance policies and accompanying guidance documents should be consolidated and clarified to be applicable to mobile devices. They should be clear, concise, comprehensive, and easy to understand and implement.

Risk Assessment Tools

Conducting regular risk assessments is an important element of any privacy management program. Adoption of new technologies to meet different business needs can introduce new and unique risks that are best identified and mitigated through the proper use of risk assessment tools. A Privacy Impact Assessment ("PIA") and a Security Threat Risk Assessment ("STRA") can help identify associated problems, or prevent them from arising in the first place.

The result of a thorough risk assessment allows public bodies to implement appropriate security safeguards and risk mitigation strategies proportionate to the sensitivity of the information stored on mobile devices.

To conduct PIAs properly, public bodies should involve the privacy officer from the outset and include all affected operational areas, including information technology managers and staff where electronic information systems are involved. The same considerations apply to conducting STRAs to assist a public

[25] The ISP notes exceptions for conducting Security Threat Risk Assessment in relation to mobile applications by referring employees to a separate guidance document titled "*Use (of) Mobile Devices and Apps in Government*". The privacy branch at the OCIO had also developed a separate PIA on mobile applications that do not use personal information, with instructions to employees on when a PIA would be necessary. Finally, the "Appropriate Use Policy" contained instructions regarding how and when to conduct PIAs when downloading mobile applications.

body in complying with security requirements under s. 30 of FIPPA. STRAs should either form a part of a PIA or be performed in conjunction with a PIA.

Recognizing the importance of STRAs, the *Core Policy and Procedures Manual* directs ministries to implement safeguards commensurate with identified risks and security requirements, and routinely review the security of its information systems.[26] In addition, the ISP included a requirement for ministries to perform a STRA prior to permitting subscription to or use of mobile computing services.[27]

Areas of Concern

Evidence of PIAs or STRAs—My investigators found that, with a few exceptions, ministries were not conducting PIAs or STRAs. The OCIO acknowledged that it was the ministries' responsibility to conduct these assessments. The ministries stated that these inadequate risk assessment practices were due to confusion around the roles and responsibilities between the OCIO and the ministries. This demonstrates how a lack of clarity can be an impediment to realizing a privacy-protective culture.

In practice, the OCIO conducts general STRAs with respect to mobile device use. This is acceptable, but individual ministries must ensure these assessments are tailored to the specific needs and vulnerabilities of their program areas. A government-wide strategy is critical to facilitate a comprehensive and coordinated approach to the protection of personal information.

I find that the selected ministries were not conducting adequate risk assessments to assist them with implementing appropriate security safeguards and risk mitigation strategies.

RECOMMENDATION 6: Government should ensure coordination between the OCIO and ministries to conduct adequate privacy and security risk assessments of employee mobile devices use.

Training

Training is necessary to effectively manage the privacy obligations related to mobile devices that access government servers. In order for a privacy management program to be effective, employees themselves must be actively

[26] Office of the Chief Information Officer–Core Policy and Procedures Manual – CPPM 12.3.6.
[27] Office of the Chief Information Officer–Information Security Policy, October 2012 – ISP 7.7.1 a.

engaged in privacy protection. *Accountable Privacy Management in B.C.'s Public Sector* states:

> Privacy training should be mandatory for all employees and should be ongoing, regular and sufficiently detailed as to equip employees with the knowledge and awareness necessary to meet privacy obligations.[28]

The ISP requires that ministries provide employees with security awareness training and ensure that employees are aware of the additional risks and responsibilities inherent to mobile computing and the use of portable storage devices.

Areas of Concern

My investigators found that ministries did undertake mandatory privacy and security training based on material developed by the OCIO. However, the training is not sufficiently customized to address the unique risks associated with the use of mobile devices.

Ongoing training is also needed to inform employees about emerging threats and best practices. Government had established centralized communication through the OCIO to inform employees of security requirements and notifications related to mobile devices, but only employees who had registered to receive such notifications would receive them. Ministry CIOs stated that they also shared security notifications from the OCIO with impacted employees by email, newsletters, and sometimes a telephone call. However, my investigators could not confirm that these alerts were timely or that they reached all affected employees.

Some ministries required that employees undertake privacy training upon hire and on an annual basis, which is commendable. Other ministries did not require regular training and with some ministries it was difficult to determine the frequency of training because they did not document training sessions.

I find that the content of training was not sufficiently detailed and customized to the specific duties of employees in relation to the use of mobile devices. Training was not conducted frequently enough in some

[28] Office of the Information and Privacy Commissioner, *Accountable Privacy Management in B.C.'s Public Sector*, p. 13 (https://www.oipc.bc.ca/guidance-documents/1545).

ministries to ensure employees are aware of their specific responsibilities and to acquire the skills necessary to fulfil their duties.

RECOMMENDATION 7: Privacy and security training should be regular and documented and specifically reference mobile devices. This training should address the responsibilities of individuals in safeguarding personal information.

RECOMMENDATION 8: Ministries should put in place a process that ensures security notifications are received by all employees who use mobile devices.

Breach and Incident Management Response Protocols

An effective privacy management program should assign responsibilities for containing, mitigating, and reporting a breach. This includes a response protocol that assigns responsibility for investigating the causes of the breach and ensuring that lessons learned are incorporated into procedures, practices, and employee training.

Personal information that resides on employee mobile devices could be the subject of a privacy breach, for instance, if the device is lost or stolen.

The B.C. government's *Process for Responding to Privacy Breaches* policy enumerates the steps that ministries must follow when responding to a privacy breach. It states that the OCIO is responsible for the coordination, investigation and resolution of breaches, and that all actual or suspected information incidents must be reported immediately to one's supervisor and to the OCIO. It also states that all incidents must be tracked by a number of different entities within government: the Privacy Investigation Unit and the Security Investigation Unit at the OCIO, the ministry CIO, the ministry information security officer, and the responsible business area.

Areas of Concern

While the general policies and processes for breach management were well documented, OIPC investigators found that compliance with the policies did not occur in all cases.

It should be noted that the OCIO provided detailed explanations of how it responds to reported incidents and breaches involving mobile devices. However, OIPC investigators did not find evidence that ministries were also involved in tracking and managing incidents and breaches. In some ministries, privacy or security officers stated they were not always notified of privacy and security incidents by the OCIO. In other ministries, those interviewed stated that the OCIO had sole responsibility for information incident management and breach reporting involving mobile devices, and would not involve the respective ministry in the breach response.

I am also troubled that my investigators found that employees often failed to immediately report lost and stolen devices as prescribed by government's *Incident Management Process*.[29] OIPC investigators found instances of employees reporting a device lost or stolen several months after the device was first noticed missing. On average it took employees two to six days to make a report. At one ministry, employees were advised not to report lost devices for up to three days in case the device was found.

OIPC investigators also found that documentation of lost and stolen devices was not properly maintained or analyzed by ministries or the OCIO, and thus the opportunity for providing these individuals with additional training was lost.

I find that government breach and incident management protocols were not consistently followed by employees.

RECOMMENDATION 9: Ministries should ensure their employees report lost or stolen devices in accordance with the OCIO's privacy and security policies and procedures.

Ongoing Assessment and Revision

As stated in my Office's guidance document, *Accountable Privacy Management in B.C.'s Public Sector*,

> To meet its FIPPA obligations and be accountable for its privacy practices, a public body should monitor, assess and revise its privacy management program regularly and consistently… in order to ensure its currency and effectiveness.

OIPC investigators found that many important elements of a privacy management program were not in place, both generally and specifically for mobile devices. At the time of this investigation, privacy officers were not designated and empowered to implement program controls that could be monitored and revised. I will monitor the progress of government in this regard

[29] B.C. Government Core Policy Chapters 12.3.6, 15.2, 20, L and OCIO *Information Incident Management Process* (IIMP).

and will report on the effectiveness of their privacy management program in future reports.

Areas of Concern

Lack of clarity regarding roles and responsibilities—A proper privacy management program clearly sets out the roles and responsibilities of those responsible for privacy within a public body. A theme that emerged throughout this investigation was confusion about the respective roles and responsibilities of the various government parties, which negatively affected mobile device management.

My investigators were told by some ministries that overall responsibility to manage the privacy and security of mobile devices lay with the OCIO. We found that the OCIO had taken on responsibility for conducting risk assessments for devices and mobile operating systems, investigating information incidents and lost and stolen devices, recommending minimum security controls for mobile devices, drafting relevant policies and procedures, and maintaining a list of employees with mobile devices connected to the mobile device management tool. However, when asked about specific inadequacies in relation to those matters, the OCIO directed my investigators back to the ministries.

The OIPC encountered this issue in a previous investigation.[30] In that report, former Commissioner Denham suggested that some functions would benefit from a government-wide approach, while others require specific knowledge about the structure, programs, personnel and information holdings of a ministry.

I support the former Commissioner’s approach on this point. Greater clarity on the roles and responsibilities of the OCIO, ministry CIOs and privacy officers would help all employees understand and contribute to effective privacy management.

I find that the selected ministries and the OCIO do not agree on where responsibility lies for the privacy management of mobile devices.

RECOMMENDATION 10: The roles and responsibilities for privacy and security management of mobile devices, including those specific to the OCIO, ministries, program areas and employees, should be clarified, documented, and effectively communicated to all responsible parties.

[30] Investigation Report F13-02: Ministry of Health; https://www.oipc.bc.ca/investigation-reports/1546.

3.2 STORAGE AND ACCESS OUTSIDE CANADA

The second objective of this investigation was to determine whether the storage of and access to personal information on mobile devices was compliant with s. 30.1 of FIPPA, which requires that personal information be stored in and accessed from Canada, unless certain exceptions apply.

Cloud computing is an internet-based service that allows a user to store and access programs and files remotely. Some mobile applications allow users to save and store information and files using cloud-based software, which are often located outside of Canada. Installing these applications may therefore result in personal information being stored or accessed outside of Canada, in contravention of FIPPA.

Areas of Concern

Compliance with Policies—The *Appropriate Use Policy*, though not specific to mobile devices, sets out restrictions on the download and use of applications. These restrictions include the requirement that employees must not download or use applications that are not available from the government approved servers and without the permission of their supervisor.

However, this policy was not enforced through technical controls and OIPC investigators were told by those interviewed that they are aware of instances where employees do not follow this policy. For example, an incident discovered in 2015 involved employees who downloaded an application for mobile devices that stored email, calendar, and contact lists to a server located outside of Canada. While this incident was investigated by the OCIO and each ministry and employee was followed up with to resolve the breach, government did not have the technical capability to detect and prevent similar incidents.

Those interviewed in the ministries told OIPC investigators that employees would sometimes report a problem associated with, or request advice about, a mobile application that was not authorized for use in government, or was not supported by the ministry. This indicates that not only are employees downloading applications that are not approved by government, but they are also not aware that they are contravening government policy.

In addition, and perhaps more troubling, government-approved and issued devices often come pre-installed with applications that include a cloud storage component. Employees commonly and quite reasonably believe that use of such pre-installed applications, and the cloud services offered by those applications, is permitted by government. However, the use of these applications is likely to contravene s. 30.1 of FIPPA.

I find that government does not have the technical capability to detect and prevent employee use of mobile applications that store personal information outside of Canada.

RECOMMENDATION 11: Government should ensure that any applications installed on government-issued mobile devices are not used to store personal information outside of Canada.

3.3 REASONABLE SECURITY ARRANGEMENTS

The final objective for this investigation was to determine whether personal information stored on mobile devices was protected against such risks as unauthorized access, collection, use, disclosure or disposal by reasonable security measures as required by s. 30 of FIPPA.

The standard of reasonableness has been interpreted in numerous investigation reports and orders.[31] The meaning of "reasonable security arrangements" can be summarized as follows:

> The reasonableness standard in s. 30 is measured on an objective basis and, while it does not require perfection, depending on the situation, it may signify a high level of rigor. To meet the reasonableness standard for security arrangements, public bodies must ensure that they have appropriate administrative, physical and technical safeguards.
>
> The measure of adequacy for these safeguards varies depending on the sensitivity of the personal information, the medium and format of the records, the estimated costs of security, the relationship between the public body and the affected individuals and how valuable the information might be for someone intending to misuse it.

Areas of Concern

Security Controls—In a report, the Auditor General explains in detail the lack of key security controls with respect to mobile devices.[32] I agree with the Auditor General's findings in that regard, and together with my findings in ss. 3.1 and 3.3 of this Report, **I find that government is not meeting its statutory obligations under s. 30 of FIPPA. I recommend that government adopt and implement all of the recommendations detailed in the Auditor General's report without delay.**

[31] OIPC Investigation Reports: F16-01, [2016] B.C.I.P.C.D. No. 5; F13-02, [2013] B.C.I.P.C.D. No. 14; F12-03, [2012] B.C.I.P.C.D. No. 7.
[32] Auditor General of B.C. – Management of Mobile Devices: Assessing the moving target in B.C. – August 2016.

4.0 SUMMARY OF FINDINGS

I have made the following findings in this investigation:

1. **I find that senior management in the selected ministries did not ensure appropriate resources were available to mitigate the specific risks associated with mobile devices, and therefore did not demonstrate sufficient commitment to a privacy-protective culture to ensure compliance with FIPPA and consistency with privacy best practices.**

2. **I find that, in the selected ministries, senior management did not adequately empower those responsible for privacy compliance.**

3. **I find that government did not have an adequate audit program in place to determine compliance with privacy obligations under FIPPA.**

4. **I find that the ministries selected for this investigation did not maintain an accurate inventory of personal information stored on mobile devices and did not categorize the sensitivity of the personal information holdings.**

5. **I find that the general nature of the ISP and the Appropriate Use Policy confused employees about their application to mobile devices. The excessive number of other policies and guidance materials made it difficult for employees to access and understand them. Therefore these policies do not fulfill the objective of providing adequate privacy protection for personal information stored on mobile devices.**

6. **I find that the selected ministries were not conducting adequate risk assessments to assist them with implementing appropriate security safeguards and risk mitigation strategies.**

7. **I find that the content of training was not sufficiently detailed and customized to the specific duties of employees in relation to the use of mobile devices. Training was not conducted frequently enough in some ministries to ensure employees are aware of their specific responsibilities and to acquire the skills necessary to fulfil their duties.**

8. **I find that government breach and incident management protocols were not consistently followed by employees.**

9. I find that the selected ministries and the OCIO do not agree on where responsibility lies for the privacy management of mobile devices.

10. I find that government does not have the technical capability to detect and prevent employee use of mobile applications that store personal information outside of Canada.

11. I find that government is not meeting its statutory obligations under s. 30 of FIPPA. I recommend that government adopt and implement all of the recommendations detailed in the Auditor General's report without delay.

5.0 SUMMARY OF RECOMMENDATIONS

RECOMMENDATION 1

Each government ministry should empower a privacy officer to develop, implement, monitor and adjust the privacy management program to the use of mobile devices. Ministries should ensure the privacy officer has adequate resources to meet privacy management responsibilities

RECOMMENDATION 2

Ministries should monitor and audit compliance with privacy policies and adopt proactive solutions to detect unauthorized use and disclosure of ministry information.

RECOMMENDATION 3

Government should review its mobile device management strategy to ensure that employees are provided with adequate training and guidance to understand the privacy and security risks posed by mobile devices.

Where strategy places too great an expectation on employee's technical knowledge, government should ensure it does not compromise the security of personal information in favour or flexibility.

RECOMMENDATION 4

Ministries should conduct a thorough review of all personal information currently stored on mobile devices and then create an inventory of the types of personal information that is commonly stored.

RECOMMENDATION 5

Compliance policies and accompanying guidance documents should be consolidated and clarified to be applicable to mobile devices. They should be clear, concise, comprehensive, and easy to understand and implement.

RECOMMENDATION 6

Government should ensure coordination between the OCIO and ministries to conduct adequate privacy and security risk assessments of employee mobile devices use.

RECOMMENDATION 7

Privacy and security training should be regular and documented and specifically reference mobile devices. This training should address the responsibilities of individuals in safeguarding personal information.

RECOMMENDATION 8

Ministries should put in place a process that ensures security notifications are received by all employees who use mobile devices.

RECOMMENDATION 9

Ministries should ensure their employees report lost or stolen devices in accordance with the OCIO's privacy and security policies and procedures.

RECOMMENDATION 10

The roles and responsibilities for privacy and security management of mobile devices, including those specific to the OCIO, ministries, program areas and employees, should be clarified, documented, and effectively communicated to all responsible parties.

RECOMMENDATION 11

Government should ensure that any applications installed on government-issued mobile devices are not used to store personal information outside of Canada.

6.0 CONCLUSION

The use of mobile devices has become essential to private and professional life. This is certainly the case in the public sector, where the administration of government is increasingly dependent on both common and novel uses of mobile technology. This investigation of government's mobile device management practice and policy and the accompanying audit conducted by the Auditor

General, have identified numerous privacy and security challenges that government must address as it develops its mobile device strategy.

The government needs to ensure that clear policies and training are in place so all employees understand their privacy and security obligations under FIPPA as they relate to mobile devices. My Office found numerous misunderstandings between ministries and the OCIO about their respective roles and responsibilities. Government can readily address these issues by implementing the recommendations contained in this report.

I am pleased that since this investigation took place, government has already taken significant steps to improve its handling of mobile devices, including the implementation of a privacy management program. Government should continue with these positive changes and fully adopt my recommendations and those in the Auditor General's Report in order to protect the personal information of its employees and citizens. My Office will follow up with government over the next year regarding its progress.

7.0 ACKNOWLEDGEMENTS

Government cooperated fully with my Office's examination.

I would like to thank the Office of the Auditor General for its work on this important issue and for working with my Office on this matter.

I would also like to thank Saloumeh Pourmalek, Policy Analyst, and Bradley Weldon, Senior Policy Analyst, who conducted this examination and contributed to this report.

October 18, 2016

ORIGINAL SIGNED BY

Drew McArthur
Acting Information and Privacy Commissioner
for British Columbia