Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

**News Release**

**For Immediate Release**
**October 18, 2016**

## Information and Privacy Commissioner calls on B.C. government to improve mobile device management

**VICTORIA**—Acting Information and Privacy Commissioner Drew McArthur recommends that the B.C. government improve its policies and practices regarding mobile device use by employees, following the release of today's report, *Mobile Device Management in B.C. Government.*

"Mobile devices are widely used to conduct government business today. When B.C. residents interact with government employees, personal information is collected – it could be emails, text messages, photos, and location information. Mobile devices are convenient, but can also be easily lost or stolen.

"Under the *Freedom of Information and Protection of Privacy Act,* public bodies have a responsibility to protect personal information. This should be a priority for the B.C. government," said McArthur.

Five ministries were selected for this investigation based on the number of devices in use and the sensitivity of the information collected and stored. Investigators from the Office of the Information and Privacy Commissioner (OIPC) examined smartphones, tablet computers, and other devices that use mobile-specific operating systems (e.g., Android, Apple iOS, or BlackBerry). The OIPC assessed government policies and practices using three criteria:

1. whether government has an effective privacy management program,
2. whether the storage and retention of personal information accessed on mobile devices occurs only in Canada, and
3. whether government has adopted reasonable security measures to protect that information.

OIPC investigators found that the numerous government policies related to mobile device use were confusing and sometimes contradictory. They also noted that, in some ministries, those responsible for privacy compliance were not adequately empowered to implement and monitor technical controls. Additionally, government did not maintain an accurate inventory of mobile devices and the personal information stored on them.

Acting Commissioner McArthur made 11 recommendations in the report, including:

- Responsibility for privacy and security management of mobile devices should be clarified, documented, and effectively communicated to all responsible parties.
- Each government ministry should empower a privacy officer and ensure that adequate resources are made available.
- Privacy and security training for government employees should be offered on an on-going basis and should specifically reference mobile devices.
- Government should ensure that employees know not to use applications on government issued mobile devices that may store personal information outside of Canada.

“Privacy management should be simple. Government employees should not have to wade through volumes of competing policies. This investigation is intended to identify potential risks before they become serious, so I have recommended some important improvements in policies, training, and risk management,” said McArthur.

“I would like to stress that this investigation was conducted at a specific point-in-time. I am encouraged that since last year, government has taken some important steps toward implementing a privacy management program.”

This investigation was unique for the OIPC, as it was conducted concurrently with an audit by the Office of the Auditor General. Each office has published a separate report, both released this morning. The OIPC and the Auditor General have also created a guidance document to help individual citizens better secure their mobile devices. It offers 15 tips on security and privacy that any mobile device user can benefit from and is available at https://www.oipc.bc.ca/investigation-reports/1993

*Investigation Report F16-03: Mobile Device Management in B.C. Government* is available for download at https://www.oipc.bc.ca/investigation-reports/1993

Commissioner McArthur and Auditor General Carol Bellringer will hold a news conference via conference call at 11:00 a.m. (Pacific Time) on Tuesday, October 18, 2016. There will be an opportunity for questions after their brief remarks.

News Conference Date: Tuesday, October. 18, 2016 Time: 11:00 a.m. (Pacific Time)
From Vancouver: 604 681-0260
From elsewhere in Canada and the USA: 1 877 353-9184
Participant Pass Code: 44848#
During question and answer period, to ask a question: Press 01
During question and answer period, to exit the question queue: Press #

Media Contact:
Erin Beattie
Office of the Information and Privacy Commissioner for B.C.
250 217-5010 | ebeattie@oipc.bc.ca
Twitter: @BCInfoPrivacy

## BACKGROUND

### Q: What was the OIPC's methodology?

The investigation was conducted between June and November 2015 and included a review of risk assessments, policies, and training materials, as well as interviews with chief information officers and other key personnel. We examined whether the management of personal information on mobile devices meets government's responsibilities under the *Freedom of Information and Protection of Privacy Act*.

Our assessment of government's management of mobile devices was based on three measures: 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.

To address the first objective, OIPC investigators evaluated whether government had key elements of a privacy management program in place by comparing government policies and practices against our 2013 guidance document entitled *Accountable Privacy Management in BC's Public Sector.* This document outlines the need for a commitment to privacy compliance, adequate program controls, and ongoing assessment and revision.

### Q. Why did the OIPC work with the Office of the Auditor General on this report?

Security and privacy are inextricably linked. Given our joint interest in mobile device management it made sense to work together.

Note that while we collected information and attended interviews together, our offices analyzed our findings separately and came to our own conclusions. The Auditor General focused more on the security of mobile devices, while the OIPC looked at privacy implications.

### Q. Did the OIPC examine the use of laptops or USB drives?

We examined devices that use mobile-specific operating systems (e.g. Android, BlackBerry, iOS). We did not look at laptops or USB drives because the risks are well understood. We did not look at wearable technology like body cameras, due to low uptake, nor flip phones because they store very little data.

### Q. How did the OIPC select the five ministries?

We wanted a representative sample of government use of mobile devices. The five ministries were selected by the Auditor General and the OIPC for several reasons, including the number of devices in use and the sensitivity of information collected and stored.