Canadian Air Transport Security Authority
Administration canadienne de la sûreté du transport aérien

Bring Your Own Device (BYOD) Program
Author: CATSA
Version: Public Summary - Privacy Impact Assessment
Date: February, 2018

Executive Summary

This is a summary of the Privacy Impact Assessment (PIA) completed by the Canadian Air Transport Security Authority (CATSA) for the Bring Your Own Device (BYOD) Program. CATSA intends to implement a BYOD Program across the organization in 2018/2019. The BYOD Program is a voluntary program which will allow CATSA employees to use their own personal mobile devices to access their CATSA email account, work contacts, and calendar.

This summary reflects the findings and recommendations of the BYOD Program PIA. The scope of this PIA was the personal information related to participating in CATSA's BYOD Program and personal information used by BYOD Participants.

The PIA examined the privacy-related impacts of the BYOD Program. The PIA concluded that CATSA has implemented risk mitigation strategies that are in line with privacy best practices including:

- Ensuring the BYOD Program participation is voluntary and based on informed consent, including requiring all Participants attend information sessions and annually update BYOD Participation Agreements;

- Establishing a flexible but enforceable suite of security policies that limits risk to CATSA and the BYOD Participants;

- Implementing a Mobile Device Management (MDM) solution to ensure policy compliance of personally owned mobile devices when connecting to CATSA IT infrastructure and to mitigate security threats;

- Enabling MDM solution features such creating a separate "container" on the personal device for CATSA data that provide security commensurate with the security classification of BYOD-related personal information (e.g., encryption, remote wipe of the container);

- Technologically limiting BYOD Participants from retaining corporate data outside the MDM's encrypted container;

- Not enabling aspects of the MDM solution that require the collection of unnecessary personal information (e.g., GPS data, personal usage details);

- Conducting a Threat Risk Assessment (TRA) to assess the threats and vulnerabilities that could affect the BYOD Program;

- Continuing to monitor the mobile threat environment for risks and vulnerabilities that could impact the BYOD Program and/or CATSA IT infrastructure; and

- Ensuring that all BYOD Participants are aware of their responsibilities stated in the CATSA Privacy Breach Response Procedure and the requirement to report lost or stolen mobile devices within 24 hours.

Privacy Principles

The findings and recommendations relating to potential privacy risks for the BYOD Program below are presented in a framework consistent with the ten privacy principles for assessing fair information handling practices.

Principle 1: Accountability

CATSA has assigned the accountability for privacy risks and their mitigation.

Principle 2: Identifying Purposes

CATSA has prepared communication material, including: mandatory information sessions to explain the privacy implications associated with the BYOD Program to employees; requiring employees to sign and annually renew Participation Agreements.

Principle 3: Consent

Participation in the BYOD Program is voluntary and based on informed consent.

Principle 4: Use

The table below illustrates the specific data elements that are used to administer the BYOD Program and by Participants in the Program:

Personal Information Elements & Source	Purpose of collection
CATSA employee • Name • Signed Participation Agreement form	• To administer BYOD Program (e.g., obtain consent from CATSA employees)
CATSA network usage details • Logs containing details of CATSA network usage	• To monitor CATSA network usage – occurs only as needed, based on analysis or reports of potential mis-use
CATSA Wi-Fi usage details • Logs containing details of CATSA Wi-Fi usage	• To monitor CATSA Wi-Fi usage – may contain identifying information
Device • IP address • Mobile device serial number • IMEI[1] • SIM • IP address • MAC address[2]	• To connect to the personally owned mobile device to push policies, e-Mail, Calendar • To confirm that • If needed, to wipe MDM Container
CATSA e-mail account (by Participants) • Email contents and attachments, calendar and contacts	• To complete duties required as CATSA employee • CATSA internal communications
CATSA e-mail account (by Participants) • Personal Information about **others** in e-mail contents and attachments, calendar and contacts	• To complete duties required as CATSA employee • As supplied by others for personal use of CATSA Participant in email, calendar and contacts

[1] International Mobile Station Equipment Identity.

[2] Media Access Control address (MAC address) - is a unique identifier associated with a network adapter. While IP addresses are associated with software, MAC addresses are linked to the hardware of network adapters. MAC addresses are used for numerous network technologies, including Bluetooth-enabled devices

Notes for Table:

1) CATSA does not collect any information related to location, personal content, or app information (other than confirmation that anything assigned by the MDM is installed and functioning).
2) CATSA has reviewed the MDM agent security and privacy setup and disabled all unnecessary collections within CATSA's control of information that may be considered personal information. Some information (e.g., IMEI, SIM Card Serial Number) is collected for comparison purposes. For example, Should a BYOD Participant put a different SIM in the phone the system would detect this and suspend the device from the BYOD Program.

Principle 5: Disclosure and Retention

Personal information collected to administer the BYOD Program must be retained for at least two years since its last administrative use. A formal retention and disposal schedule will be established in consultation with CATSA's Information Management.

Principle 6: Accuracy

CATSA BYOD Participant-related personal information is voluntarily provided to CATSA directly from the individual to whom it pertains.

Principle 7: Safeguarding

Prior to the launch of BYOD Program, CATSA officials conducted a TRA. CATSA is satisfied that the administrative, physical and technical safeguards associated with the BYOD Program are commensurate with the sensitivity of personal information associated with the Program.

Principle 8: Openness

CATSA is posting this summary of the BYOD PIA on the CATSA website.

Principle 9: Individual Access

Individuals requesting access to their personal information collected for the BYOD Program may contact the CATSA Access to Information and Privacy Coordinator.

Principle 10: Challenging Compliance

Individuals requesting additional information regarding the privacy management features of the BYOD Program may contact the CATSA Privacy Advisor at priv@catsa.gc.ca.

Conclusion

In conducting interviews and reviewing the documentation provided for PIA purposes, it was concluded that CATSA has incorporated privacy as a core element of the BYOD Program and will continue to do so.