Full Body Scanner Privacy Impact Assessment (revised)

Author: CATSA
Version: Summary - Privacy Impact Assessment
Date: January 2017

Executive Summary

This is a summary of the Privacy Impact Assessment (PIA) completed by the Canadian Air Transport Security Authority (CATSA) for the Full Body Scanner (FBS) Primary.

FBS detect both metallic and non-metallic threats, providing a more complete security screening than Walk-Through Metal Detectors (WTMDs). Currently, FBS units are used for secondary screening. In order to more fully utilize these important tools for the protection of Canadian air travelers, CATSA is testing a change to current screening process which will use FBS units in the primary screening position at certain checkpoints, where they will used instead of a WTMD.

FBS use remains voluntary. All individuals assigned to a line using FBS Primary will have the option of a physical search of person instead of FBS. Any individual who cannot participate in FBS Primary screening (for reasons of physical incapability of assuming the arms-lifted position necessary for the scanning, or due to insufficient height) will be screened with the WTMD.

This summary reflects the findings from the FBS Primary PIA. The PIA was conducted using the Treasury Board of Canada Secretariat guidelines for conducting PIAs, which incorporates the ten principles of the Canadian Standards Association Model Code for assessing fair information handling practices.

The PIA concluded that CATSA is addressing all risks with risk mitigation strategies that are in line with privacy best practices including:

- ensuring the FBS process remains anonymous and voluntary;

The protections provided by the earlier addition of Automatic Threat Recognition (ATR) software (see FBS PIA Update, 2013) are retained:

- eliminating the requirement for an ISO to view a mmW image of a passenger;
- not correlating the raw data in any way with the name of the passenger or any other identifying information;
- ensuring that the FBS system is “stand-alone”;
- ensuring that the raw data cannot be accessed or retained;
- ensuring that the FBS unit is configured not to store, print, transmit, or save raw data;
- ensuring passengers are provided with an opportunity to divest any items that may trigger an ATR alarm before they enter the FBS unit;
- ensuring the FBS unit is configured not to create mmW images of passengers; and
- permitting only qualified Screening Officers to operate FBS units equipped with ATR software.

Privacy Principles

The findings and recommendations relating to potential privacy risks for the FBS Primary PIA are presented in a framework consistent with the ten privacy principles of the CSA Model Code 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 will continue to make information accessible to passengers at the checkpoint and online explaining the option to have a physical search of person instead of FBS. The FBS units equipped with ATR software will continue to operate without retaining any personally identifiable information. The FBS units are configured to permanently delete the raw data and the “stick” figure image immediately after the FBS screening process is complete.

Principle 3: Consent

CATSA will continue to offer passengers a choice between FBS and a physical search. CATSA will ensure that passengers are provided with adequate information relating to FBS, the change to FBS Primary and ATR software at the PBS checkpoint and online.

Principle 4: Use

The FBS units equipped with ATR software will use raw data for the specific purpose of identifying anomalies on passengers. This non-identifiable data is immediately and permanently deleted after the screening process is completed.

Principle 5: Disclosure and Retention

The FBS units equipped with ATR software will continue to operate without disclosing or retaining any personally identifiable information.

Principle 6: Accuracy

In an effort to improve the accuracy of the ATR readings, passengers, before they enter the FBS unit, are provided with an opportunity to remove any items that may trigger an alarm. Should the ATR detect an alarm, passengers are provided with a second opportunity to remove any items that they may have overlooked, before they receive a second FBS scan.

Principle 7: Safeguarding

CATSA is satisfied that the risk to privacy is substantially mitigated, as the ATR software does not require the collection of any identifiable information other than the passenger’s transitory raw data, which is immediately and permanently deleted after the screening process is completed. CATSA will regularly subject the FBS units equipped with ATR software to technical audits to ensure that all settings and configurations have not been modified or changed.

Principle 8: Openness

CATSA will continue to ensure that information explaining how the ATR software works is readily available to the public. (See FBS information on the CATSA website and the FBS Info Card.)

Principle 9: Individual Access

As the FBS units equipped with ATR software do not retain any identifiable information, CATSA will not be able to provide an individual with access to their personal information.

Principle 10: Challenging Compliance

Individuals requesting additional information regarding the privacy management features of ATR software may contact the CATSA Privacy Advisor at priv@catsa.gc.ca. Individuals who are not satisfied with CATSA’s response may direct their complaints to the OPC.

Conclusion

In January 2017, CATSA submitted a copy of this PIA to the OPC and we await their comments. Following OPC comments on previous FBS PIAs, CATSA has been monitoring passenger complaints since the activation of FBS ATR in April of 2013 and there has been no notable privacy concerns expressed.