IN BRIEF

Parliamentary Information and Research Service
Library of Parliament

Allison Padova
28 July 2004

Airline Passenger Screening in the United States and Canada – Developments Since September 2001

INTRODUCTION

Aviation security has been a major concern in the United States, and indeed around the world, since the terrorist attacks of 11 September 2001. The attacks, for which commercial airliners were hijacked and used as weapons against the general public, made it clear that it was no longer sufficient to screen only the objects brought on board aircraft. Security officials now believe, given the heightened threat environment, that screening *people* boarding commercial aircraft has become essential.

In November 2001, the United States passed legislation authorizing an automated passenger screening system. The computer-assisted passenger pre-screening system (CAPPS II), which will replace an existing CAPPS system administered by airlines, is currently under development.

In Canada, the *Public Safety Act, 2002* includes provisions that would allow authorities to screen airline passengers for the first time. The Act received Royal Assent in May 2004.

This paper describes the U.S. system of passenger screening under development, and outlines the general framework of the regime that is expected to be implemented in Canada under the *Public Safety Act, 2002*. The Canadian program would be similar to CAPPS II in that it would compare airline passenger data against government information to prevent suspected terrorists and certain fugitives from boarding airplanes. Given the similarities between the two systems, it is not surprising that the criticisms of the system in the United States are largely echoed in Canada. Key concerns are summarized in this paper. To the extent that they are known, the key differences between the U.S. and Canadian approaches to airline passenger screening are also indicated.

AIRLINE PASSENGER SCREENING IN THE UNITED STATES

Section 109 of the Aviation and Transportation Security Act (P.L. 107-71), signed into law on 19 November 2001, authorizes the Under Secretary of Transportation for Security to take certain actions to enhance transportation security. Subsection 109(a)5 provides for the use of technology to enable the communication of threats to aid in the screening of individuals on airport property who are identified in security-related databases. The Transportation Security Administration's (TSA) response to this provision was to start developing CAPPS II in March 2003 to replace the current CAPPS. The purpose of CAPPS II is to minimize threats to passenger and aviation security by determining which passengers should be afforded additional scrutiny prior to boarding an aircraft.

CAPPS II is intended to operate using the home phone number, address, name and date of birth of all air travellers to, from and within the United States when they book their travel. Companies running the airlines' computerized reservation system are expected to transmit data to the TSA. The TSA plans to first check the data outside of a government firewall against private, commercial databases to verify passenger identities. No information contained in the commercial databases should be brought into the government's system.

Once CAPPS II has authenticated a passenger's identity, it would conduct a risk assessment. The assessment is expected to determine the likelihood that a passenger is a known terrorist, or has identifiable links to known terrorists or terrorist organizations. The risk assessment would involve highly classified algorithms and be conducted internally within the U.S. government.

CAPPS II is also expected to perform a check against lists of terrorists and known or suspected threats, to detect individuals who may pose a terrorist-related threat or who have outstanding state or federal warrants for crimes of violence.

CAPPS II should code passengers with risk levels: green (low), yellow (uncertain) or red (identified risk). These colours would indicate to screeners whether to let passengers through with minimum scrutiny (green), subject passengers to a heightened level of scrutiny (yellow) or call law enforcement agents (red). The system is intended to reduce dependency on random passenger selection for additional screening, and is expected to reduce the inconvenience for the vast majority of passengers who are low-risk.

CAPPS II is being developed in a nine-increment process that began in March 2003. The first two increments were completed by October 2003; however, they have not yet been completely tested. Privacy concerns of air carriers in the United States and foreign governments have prevented the TSA from obtaining the necessary passenger data to test the system. Due to the postponement of tests using historic airline data, all other increments have been delayed and the TSA is uncertain when the system will be ready to receive live data from airlines.

The U.S. General Accounting Office has noted that the development of the system is behind schedule and continues to face numerous challenges that could affect the successful development and implementation of CAPPS II. These include the Congressional requirement that the TSA address seven outstanding issues related to the development, operation and public acceptance of the system. These are:

- Accuracy of data;
- Stress testing;
- Abuse prevention;
- Unauthorized access prevention;
- Policies for operation and use;
- Privacy concerns; and
- Redress process.

The TSA is planning to implement CAPPS II after it completes the system testing, which will depend on timely international cooperation, and after it meets the Congressional requirements. It is not certain whether these steps will be achieved in 2004.

AIRLINE PASSENGER SCREENING IN CANADA

The Canadian government plans to undertake airline passenger screening to identify terrorists and outstanding warrants for specified, serious crimes. The *Public Safety Act, 2002* adds a new section to the *Aeronautics Act* for this purpose.

Section 4.82 of the *Aeronautics Act* authorizes the Commissioner of the RCMP, the Director of CSIS and other designated persons to require passenger information from air carriers and operators of airline reservation systems. Up to 34 elements of passenger information can be used for purposes of: transportation security; national security investigations relating to terrorism; situations of immediate threat to life or safety of a person; enforcement of Canada-wide arrest warrants for offences punishable by five years or more of imprisonment; and certain arrest warrants under the *Immigration and Refugee Protection Act* and the *Extradition Act*. If there is an immediate threat to transportation security or the life, health or safety of a person, the information may be disclosed to any person in a position to respond to the threat or needing the information to respond to a threat, domestically or internationally.

Airlines and airline reservation systems are expected to provide a continuous feed of airline passenger data that will be compared against security and intelligence databases by computer for these purposes.

Public Safety and Emergency Preparedness Canada (PSEPC), which oversees the RCMP, is currently preparing an implementation plan for Cabinet. The plan must receive Cabinet approval, and PSEPC has not set a date for the roll-out of section 4.82.

KEY DIFFERENCES BETWEEN U.S. AND CANADIAN METHODOLOGIES

Many of the Canadian system's operational aspects remain to be determined. However, a few key differences between the Canadian provisions and the U.S. program already under development may be noted at this time.

In contrast to the U.S. system, the Canadian legislation:

- Has no provisions related to verifying passenger identities using commercial databases or otherwise.

- Assigns designated CSIS and RCMP officers – not a computer algorithm – to determine the threat posed by a match between government databases and the passenger list to transport or national security.

- Provides that *unmatched* passenger information must be destroyed within seven days, whereas unmatched information on citizens in the U.S. system is expected to be destroyed immediately after the passenger's itinerary is completed.

  Matched passenger information may be retained in Canada as long as it is reasonably required for the purposes of transportation security or an investigation into national security. Records must be kept to justify retention. In the United States, matched domestic information is expected to be kept for seven years and foreign information would be kept longer.

- Contains no authority for designated CSIS or RCMP officials to make blanket disclosures of information, whereas the TSA has submitted a proposed rule to the Federal Register exempting CAPPS II from the U.S. Privacy Act. This would permit the TSA to disclose information to third parties for any purpose.

- Contains privacy safeguards in the form of written retention and disclosure records, thresholds of suspicion for disclosure, and restricted access to the data. The TSA has proposed no privacy safeguards to date.

COMMON CONCERNS

While the public security goal of CAPPS II in the United States and the airline passenger screening provisions in Canada's *Public Safety Act, 2002* is widely supported in principle, the proposed systems' similar approaches to achieving that goal have drawn strong criticism from privacy activists, civil libertarians, legal experts and other groups in both countries.

Critics in the United States and Canada generally oppose the same aspects of their respective systems. They liken them to "internal border control" systems that unduly compromise an individual's right to anonymity before the state and the right to be presumed innocent. The risk of "mission creep," whereby the list of individuals targeted by the system expands, is also a concern of these groups. These groups and others have identified the potential for errors to exist in databases and a person's inability to easily correct them. The possibility that information contained in databases and transferred between them may be vulnerable to unauthorized access is also a concern. Finally, the weakness of these systems against identity theft and their susceptibility to racial bias have been highlighted.

CONCLUSIONS

Privacy activists and other groups have presented strong arguments against passenger screening initiatives in the United States and Canada. Nonetheless, the governments of these two countries, and others, have responded with conviction that the terrorist attacks of 11 September 2001 have necessitated a shift in the balance between individual and collective rights. Their view is that certain intrusions into individuals' privacy are justified, given the potential for future terrorist acts to threaten public security.

Australia, the United Kingdom, Korea and other countries are currently contemplating and/or planning passenger screening systems.

In light of the ongoing debate on this issue, particularly in the United States, a supplementary publication entitled *Airline Passenger Screening in the United States – Update* will be issued by the Library of Parliament in the fall of 2004.