Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

# The Privacy Implications of Aviation Security Measures

## Office of the Privacy Commissioner of Canada's Submission in Response to the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182

November 6, 2007
Ottawa, Ontario

Jennifer Stoddart
Privacy Commissioner of Canada

**Table of Contents**



**Enclosures**

**Tab A:** Solicitor General of Canada, *Bill C-17 (Public Safety Act): RCMP and CSIS Access to Airline Passenger Information* – November 6, 2002

## 1. Introduction

On May 1, 2006, an Order in Council was issued creating the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182. As part of its terms of reference the Commission of Inquiry was asked to make findings and recommendations with respect to several matters, including "whether further changes in practice or legislation are required to address the specific aviation security breaches associated with the Air India Flight 182 bombing, particularly those relating to the screening of passengers and their baggage."

The Commission of Inquiry has asked the Office of the Privacy Commissioner of Canada to comment on the privacy implications of various government programs that have been introduced to enhance aviation security.

Many measures have been introduced in Canada and elsewhere in the wake of the Air India bombing, other incidents such as the bombing of Pan Am Flight 103, and more recently, the terrorist attacks of September 11, 2001. While the recently implemented Passenger Protect Program (PPP) has received a great deal of attention, it is only one of several programs intended to enhance aviation safety and national security that involve the collection, use and disclosure of personal information or otherwise raise privacy concerns.

Most of our comments relate to the PPP but before discussing this program we will comment briefly on several other aviation security measures that raise privacy concerns. This will help put our comments on the PPP in context.

## 2. Advance Passenger Information and Passenger Name Record (API/PNR) Program

This program involves the collection of Advanced Passenger Information (API) and Passenger Name Record (PNR) information from all air carriers arriving in Canada.

The purpose of the API/PNR Program is to identify persons (passengers or crew members) prior to their arrival in Canada who may pose a risk to the safety and security of Canada. Although this program primarily serves border control purposes, the program also relates to aviation security.

API consists of information—name, date of birth, gender, citizenship, and passport, visa or alien resident number—that is found on a passport or equivalent travel document. PNR information consists of a large number of data elements, including information about the travel agent, the manner in which the ticket was paid for, the number of bags checked and the baggage tag numbers, meal preferences or other special requests, the class of service, whether the ticket was paid for by someone other than the ticket holder, the itinerary, and various dates (when the ticket was issued, date of travel, etc.) that is contained in an airline reservation system. Air carriers are required to provide this information electronically in advance of the arrival of the flight. This information is retained by CBSA for 3.5 years.

Canada's API/PNR program is authorized under the *Customs Act* (Bill S 23), which received Royal Assent on 25 October 2001 and the *Immigration and Refugee Protection Act* (IRPA). API has been collected by the CBSA since October 7, 2002. The PNR program was implemented on July 8, 2003.

Our Office raised several concerns when the API/PNR program was initially proposed.[1] We were particularly troubled by the creation of a database containing extensive information on the foreign travel activities of all law-abiding Canadians that, under the information-sharing provisions of the *Customs Act*, would have been available for a virtually unlimited range of governmental and law enforcement purposes. Some of our concerns were addressed, for example, by shortening the period of retention and by limiting the purposes for which the information could be used.

API/PNR information is shared with the United States under item 8 of the Canada-U.S. Smart Border Declaration. More specifically, the two countries have agreed to share API and PNR information on high-risk travellers destined to either country using a jointly developed risk scoring mechanism. The United States has a similar program that requires air carriers to provide API/PNR information electronically in advance of the arrival of the flight. Bill C-44 was passed in late 2001authorizing Canadian air carriers to divulge passenger information to the customs and immigration authorities of a foreign state.

An automated process to share information between the two countries on suspected high risk travelers was implemented on February 6, 2004. The sharing of this information is managed on a 24/7 basis through Canada's National Risk Assessment Centre and the U.S. National Targeting Center. Our understanding is that information is shared selectively on a "need to know" basis.

### 3. CANPASS Air and NEXUS

CANPASS Air allows pre-approved, "low-risk" air travellers entering Canada to clear customs and immigration by going to a kiosk, presenting their CANPASS card and looking into a camera that verifies their identity using the iris as an identifier. The program is relevant to aviation security and national security because it allows CBSA officers to concentrate their efforts on unknown or high-risk travellers and goods.

The legislative authority for the CANPASS programs is found in Section 11.1 of the *Customs Act.* That section allows the Minister of National Revenue, subject to the regulations, to issue authorizations to persons that will enable them to present themselves in alternative manners.

The CANPASS Application Form (used for CANPASS Air, CANPASS Corporate or Private Aircraft or CANPASS Private Boat) requires name, address, gender, date of birth, contact information, proof of citizenship and employment history for the past 5 years and a declaration regarding customs or immigration violations, or criminal offences for which a pardon has not been granted. Upon receipt of a CANPASS application, CBSA conducts a risk assessment that involves a rigorous background and security clearance check of all applicants. During the risk assessment, applicants are checked against a number of law enforcement, customs and immigration databases to ensure that they are eligible for the program. Each member's eligibility is re-assessed annually.

[1] See, for example, Commissioner Radwanski's September 26, 2002 letter to The Honourable Elinor Caplan, Minister of National Revenue - *http://www.privcom.gc.ca/media/nr-c/02_05_b_020926_3_e.asp*

NEXUS is a somewhat similar “trusted traveler” program. Like CANPASS it also has a highway and a marine component and it uses the iris as a means of authenticating identity.

One significant difference is that NEXUS is a joint Canada-United Sates program that is open to citizens and selected non-citizen residents of both countries. As well, it facilitates quicker entry into both the United States and Canada while CANPASS can only be used to enter Canada. The NEXUS program flows from the *Canada-United States of America Accord on Our Shared Border* and is an initiatives of the Smart Border Declaration's 32-Point Plan

In addition to the personal information provided by the applicant and the information obtained as part of the security background checks, the program also involves the collection of a fingerprint biometric of the applicant’s two index fingers and a digital photograph of the face.

The privacy concerns raised by the programs are mitigated somewhat by their voluntary nature.

## 4. Prescreening of Passengers

Screening of passengers is conducted by the Canadian Air Transport Security Authority (CATSA.) The purpose of the program is to screen passengers and carry-on baggage for prohibited items or dangerous goods (e.g., weapons, explosive substances.) Although the program does not typically involve the collection of personal information it does raise privacy concerns because the traveller may be subjected to invasive searches of the person and his or her baggage.

We are aware that there are technologies available such as backscatter x-ray technology and millimeter wave technology that can “see through” clothing to detect weapons and other dangerous items. We have not examined these technologies in any detail. Our sense is that there is a range of views on the privacy implications of these technologies. Some people believe that they are less intrusive than a “pat-down” because they do not involve any physical contact; others perceive them to be more intrusive because they generate an image of the essentially naked human body. We would recommend that if these technologies are introduced in Canada that they should be used as selectively as possible and that travellers be given the option of a physical search.

To date, the prescreening of passengers by CATSA has involved the screening of carry on baggage and screening passengers to ensure that they are not carrying dangerous or prohibited items. CATSA agents also ensure that the passenger has a boarding pass.

However, there seems to be pressure to adopt measures that place more emphasis on identity screening and the collection of information about travellers. The Passenger Protect Program is one obvious example and, as discussed below, we understand that CATSA is exploring screening methods that involve the collection of personal information.

CATSA has recently implemented a pilot project with one air carrier that involves new “2 D” boarding passes that contain a scanable barcode.[2] One purpose of the scanning is to detect forged or fake boarding passes. However, we understand that the scanning will also capture

[2] CATSA’s web site contain a brief description of this project - http://www.catsa-acsta.gc.ca/english/travel_voyage/calgary.shtml

several pieces of personal information including the passenger's name and flight number and this information will be retained until the flight departs the airport. At present, CATSA does not collect any personal information about the passengers it screens. In fact, CATSA does not know who is in the airport. This will change if this project is implemented although CATSA has assured us that this identifying information will only be used in the event of an incident.

We do not know if forged and fake boarding passes pose a risk; to the extent that they do, this program might help to address this security risk. The purpose or rationale for collecting personal information from boarding passes is much less clear.

This move towards identity screening is troubling from a privacy perspective because it creates the potential for increased monitoring and surveillance. As more agencies collect more personal information about our travelling patterns it will become increasingly easy to track our movements. In addition, identity screening places increased emphasis on the integrity of the authentication documents, potentially leading to the need for greater and more intrusive authentication procedures or for a universal form of identification such as a national identity card. In other words, identity screening can lead to other privacy invasive measures.

## 5. Restricted Area Identification Card (RAIC)

The purpose of this program is to enhance airport security by ensuring that individuals accessing restricted airport zones are authorized to be in the restricted area.

This is an identification program that requires airport workers, with authorized access to restricted airport areas, be issued a biometric card called the RAIC. The RAIC uses two kinds of biometric data—fingerprint and iris patterns—to authenticate a person's identity. Scanners are used to check one of the two physical characteristics of the cardholder with the templates stored in the card's computer chip. The card's validity is also verified against a national database.

In addition to the collection of two biometrics, the program involves the collection of personal information necessary to allow Transport Canada to issue a security clearance.

## 6. The Passenger Protect Program

### 6.1 The Rationale for the Program

The Office of the Privacy Commissioner of Canada submitted 24 questions to Transport Canada in August 2005 concerning the Passenger Protect Program.[3] The first question dealt with the rationale or justification for the Program:

> What studies, if any, has the department carried out to demonstrate that advance passenger information will be useful in identifying high-risk travellers?

Transport Canada's response did not really answer the question:

[3] The Questions and Answers can be found at - http://www.tc.gc.ca/vigilance/sep/passenger_protect/Q&A.htm#1

> The Passenger Protect Program proposes to use a watchlist to prevent specified individuals from boarding flights based on practical global experience and risk assessment rather than specific studies. Watchlists are used worldwide to protect the public from the actions of certain individuals. Border agencies, for instance, have stopped numerous dangerous individuals from crossing borders. The Canadian Border Services Agency uses Advance Passenger Information for air passengers already, to great benefit, to intercept dangerous individuals once a flight has landed in Canada. Passenger Protect will use a limited amount of Advance Passenger Information, with respect to specified individuals, to stop individuals who pose a risk to a flight from boarding the flight.

We have suggested that when introducing measures that intrude on privacy the government should ask four questions:

- Is the measure demonstrably necessary in order to meet some specific need?
- Is it likely to be effective in achieving its intended purpose?
- Is the intrusion on privacy proportional to the security benefit to be derived? and
- Is it demonstrably less privacy invasive than other measures that would achieve the same purpose?

We do not question the need to enhance aviation security, but it is not clear to us that the PPP is demonstrably necessary, that it is likely to be effective or that it is proportionate to the security benefit. Attempting to answer these questions is difficult because the rationale for the program is not clear. In particular, the notion that there are individuals who pose an imminent threat to aviation security but who have not committed any acts that warrant arrest is difficult to understand. As Professor Lyon put it when he appeared before the Commission of inquiry, there is a built in tension in the Specified Persons' List because it consists of "people who are too dangerous to fly, but too innocent to be arrested."[4] Furthermore, it consist of people who are considered too dangerous to fly who are permitted to use other forms of transportation and attend events where large numbers of people are likely to be present.

We are not alone in questioning the rationale and effectiveness of the Program. Two of the experts on aviation security who appeared before the Commission of Inquiry expressed similar reservations.

Dr Sweet, an Associate Professor at the University of Connecticut and retired Lieutenant Colonel from the U.S. Air Force, stated that she is not a proponent of no-fly lists, "I don't think it works". She went on to suggest that "it's too hard to separate people with the same names … you might do a great job in catching people who are maybe trying to escape an arrest warrant, but you're probably not going to catch a lot of terrorists."[5]

In response to a question about his views on the PPP in particular and no-fly lists in general, Mr Rodney Wallis, an aviation expert from the United Kingdom stated

[4] Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, Transcripts of Public Hearing, Volume 40, June 5, 2007, p.4858.
[5] *Ibid*., Volume 41, June 6, 2007, p.4980.

> "I am not in favour. I think the whole thing is very peripheral as far as security is concerned. I had problems listening to the testimony yesterday. Somehow I felt -- I was left with the impression that the program hadn't been adequately researched or thought through."[6]

In terms of less privacy invasive alternatives, we are not experts in aviation security, but based on our general understanding and the testimony before this Commission there would appear to be several ways of increasing aviation security that do not involve the collection of large amounts of personal information, for example

- Checking the baggage of passengers who are perceived to pose a threat;
- More thorough screening of cargo;
- Greater use of air marshalls—our understanding is that air marshals are placed on specific flights, e.g., to Reagan Airport in Washington, as a matter of course and that marshalls are placed on other planes based on a risk assessment;
- Improved security awareness training for all airport personnel;
- More rigorous baggage reconciliation; and
- Stricter access controls to sensitive areas.

We are not suggesting that any of these measures alone are adequate. We understand the notion that security has to consist of several layers. We would recommend that security measures that have little or no impact on privacy be fully explored before introducing measures that are more privacy invasive.

### 6.2 The Legislative Authority for the Program and Parliamentary Consideration of the PPP

The "Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials Passenger Protect Program – Canada's Aviation No-fly List" issued on June 28, 2007 states:

> "The *Aeronautics Act* does not provide a clear or adequate legislative framework to support the Passenger Protect Program as it has been described by Transport Canada in the Regulatory Impact Analysis Statement accompanying the Identity Screening Regulation."[7]

The resolution was not intended to suggest that Transport Canada did not have the legislative authority to introduce the PPP. Rather, as we will discuss below, this statement was intended to highlight a lack of clarity and detail in the legislation and the accompanying regulations.

According to Transport Canada, the legislative basis for the PPP is found in a series of provisions in the *Aeronautics Act* (ss. 4.72, 4.76, 4.77, 4.81, 4.82 and 4.85 (1) and (3)). These

---

[6] *Ibid.*, Volume 41, June 6, 2007, p. 5020.

[7] *Resolution of Canada's Privacy Commissioners and Privacy Enforcement Officials Passenger Protect Program – Canada's Aviation No-fly List,* June 28, 2007 **-** http://www.privcom.gc.ca/nfl/res_20070628_e.asp

provisions were added to the *Aeronautics Act* by the *Public Safety Act*. The *Public Safety Act* was first introduced as Bill C-42, which received first reading in November 2001, shortly after the terrorist attacks of September 11, 2001. C-42 was withdrawn in response to significant criticism, revised somewhat, and reappeared as Bill C-55. C-55 died on the Order Paper when Parliament prorogued in September 2002. Bill C-17, its successor, also died on the Order Paper. C-7 was introduced on February 11, 2004 it and received Royal Assent on May 6, 2004.

During the two and a half year period between the introduction of the legislation and Royal Assent, the *Public Safety Act* was the subject of a great deal of public and Parliamentary scrutiny. However, during this time, the possibility that the amendments to the *Aeronautics Act* listed above would be used to authorize the PPP does not appear to have been discussed publicly.

We have gone back and looked at the following testimony:

- Elinor Caplan, Minister of National Revenue, and staff members before the House Legislative Committee, December 10, 2002;
- Wayne Easter, the Solicitor General of Canada, Commissioner Zacardelli of the RCMP, Ward Elcock, the Director of the Canadian Security Intelligence Service (CSIS), and staff members before the House Legislative Committee, December 5, 2002;
- John McCallum, Minister of National Defence, and staff members before the House Legislative Committee, December 10, 2002; and
- The testimony of John Read, Director General at Transport Canada and officials from various other departments before the Senate Standing Committee on Transport and Communications, Match 26, 2004.

These witnesses did not raise the possibility that the government intended to introduce a no-fly program.

In fact, information provided in the Solicitor General's web site (see Tab A), dated November 6, 2002 specifically states:

> "This Bill [C-17] does not compel passengers to identify themselves to the police or to provide personal information to the airlines. As is the case now, this personal information is provided voluntarily. After this information is matched against intelligence under the control of the RCMP and CSIS, designated officers would be able to use it to identify risks to transportation and national security."

While it is true that the *Public Safety Act* does not directly compel passengers to identify themselves, the regulations issued pursuant to the amendment to the *Aeronautics Act* that were introduced in the *Public Safety Act* do compel passengers to provide personal information to the airlines.

Nor did our Office raise the possibility that a no-fly program would be introduced either in our public comments on the various iterations of the *Public Safety Act* or when Commissioner Radwanski appeared before the House of Commons Legislative Committee on Bill C-17 on February 6, 2003 or before the Subcommittee on National Security of the Standing Committee on Justice and Human Rights on February 10, 2003 or when Commissioner Stoddart appeared before Senate Standing Committee on Transport and Communications to comment on Bill C-7 on March 18, 2004.

Our comments and the comments of many other interested parties focused on section 4.82 that permit the Commissioner of the Royal Canadian Mounted Police (RCMP), the Director of the Canadian Security Intelligence Service (CSIS) to require air carriers and operators of reservation systems to provide certain passenger information that can be used and disclosed for a number of purposes including purposes unrelated to national security or aviation safety such as the enforcement of arrest warrants for offences punishable by five years or more of imprisonment and that are specified in the regulations; and arrest warrants under the *Immigration and Refugee Protection Act* and the *Extradition Act*. Our Office would certainly have addressed the issue if we were aware that the legislation would be used to introduce a "no-fly" program.

We were first briefed on the proposed program in September 2004, shortly after the *Globe and Mail* carried a story about Transport Canada's plans to develop a "no-fly" list.

The significance of the timing is that Transport Canada announced its intention to introduce the Passenger Protect Program after the legislative changes underlying the Program were passed by Parliament. Thus, neither the public nor Parliament had a meaningful opportunity to question or challenge the legislation authorizing the Program.

This is one of the reasons why the resolution signed by Canada's privacy commissioners and privacy enforcement officials recommended that the Program be referred to a Parliamentary committee for comprehensive public scrutiny and debate. Parliament should review the justification for the program, the operation of the program, the impact on fundamental rights and freedoms and the adequacy of the current legal framework.

### 6.3 The Creation of the Specified Person List

According to information posted on Transport Canada's web site an individual will be added to the specified persons list (SPL)

> "if the person's actions lead to a determination that the individual may, should they be permitted to board an aircraft, pose an immediate threat to aviation security, including:
>
> - An individual who is or has been involved in a terrorist group, and who, it can reasonably be suspected, will endanger the security of any aircraft or aerodrome or the safety of the public, passengers or crew members
> - An individual who has been convicted of one or more serious and life-threatening crimes against aviation security

- An individual who has been convicted or one or more serious and life-threatening offences and who may attack or harm an air carrier, passengers or crew members." [8]

This sets out three criteria that will be used by the Advisory Group, chaired by Transport Canada, to determine if an individual may pose "an immediate threat to aviation security. The second of the criteria is the clearest since it seems to involve a question of fact. The first and third criteria are less clear because they explicitly involve a judgment. They also seem to involve a two-part test; however, it is difficult to know how to interpret these criteria. For example, is there an automatic assumption that anyone "who is or has been involved in a terrorist group" is automatically judged to be a threat to an aircraft? Or, should these guidelines be interpreted to mean that individuals cannot be added to the SPL unless they have been convicted of a serious offence, including an offence against aviation security, or has been involved in a terrorist group? With respect to the first criterion, what does it mean to be or have been "involved in a terrorist group"? Again, this seems to involve a judgment rather than a question of fact.

Nor is it clear that these three criteria are the only factors that will be used. The use of the term "including" suggests that these may in fact not be the only criteria that the Department can use to add someone to the SPL. In his testimony before this Inquiry, Mr. Brandt, Director of Security Policy at Transport Canada, suggested that the Minister could consider other factors and that his discretion could not be limited by the guidelines:

> "The authority of the Minister, the legal authority of the Minister to prevent someone from boarding an aircraft is very broad. So the legal justification is really in the development of the program. These guidelines indicate, you know, this is what would be used but that does not fetter the discretion of the Minister either.[9]

We can appreciate that it would be difficult to develop hard and fast rules about who will be included on the SPL, but the listed criteria leave a great deal of room for discretion. That these criteria are simply guidelines as opposed to regulations further increases their discretionary nature.

The clarity of the criteria is important for two reasons:

- They are the only information that an individual can use to attempt to determine if he or she is on the SPL; and
- It will be more difficult for an individual to challenge his or her inclusion on the SPL based on such broad criteria.

Clearer, more specific criteria set out in regulations would be an improvement.

### 6.4 The Role of the RCMP and CSIS

The decision to add someone to the SPL is made by the Minister of Transport based on advice received from an Advisory Group. The Advisory Group is advised by the Department of Justice

[8] See http://www.tc.gc.ca/vigilance/sep/passenger_protect/menu.htm#Identity%20Screening%20Regulations,
[9] Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, Transcripts of Public Hearing, Volume 40, June 5, 2007, p.4876.

and includes a senior officer from the Canadian Security Intelligence Service (CSIS), a senior officer of the Royal Canadian Mounted Police (RCMP), other Transport Canada officials as required and representatives from any relevant Canadian government department or agency as required.

The RCMP and CSIS play a dual role in the creation of the SPL: they will identify and provide information about potential candidates for the SPL; and, as members of the Advisory Committee, they will provide input into the decision to add individuals, based primarily on information they have provided. Given the significance of the SPL and the potential impact on individual that could arise from the use of incomplete or inaccurate information, some of which will be derived from foreign sources, the decision to list an individual should be based on a rigorous evaluation of the information provided by the RCMP and CSIS. However, with these two agencies on the Advisory Group one has to question whether this will occur.

We are also concerned about the possibility that the RCMP and CSIS will, in turn, be able to use information obtained as part of the PPP process for purposes unrelated to aviation security. Section 4.82 of the A*eronautics Act* provides Transport Canada with the authority to disclose information received by air carriers subsequent to an SPL match to the RCMP and CSIS.

Our understanding is that when an emergency direction is issued, Transport Canada will contact the RCMP's National Operations Centre (NOC) and possibly CSIS. Transport Canada may also provide the RCMP and CSIS with additional information obtained from an air carrier over and above that needed to confirm an individual's identity, for example, that the individual was attempting to fly to a certain destination or that the individual was traveling with another person. This is information that Transport Canada can obtain from airline reservation systems under the authority granted by the *Aeronautics Act.*

There does not seem to be anything preventing the RCMP or CSIS from using this information for purposes unrelated to aviation security, assuming of course the purposes are within their mandates. As a result, information that is obtained through the PPP could result in individuals, their families, and acquaintances being targeted by law enforcement officials for surveillance for reasons unrelated to aviation security. For example, as a result of an individual being denied boarding, the RCMP and possibly CSIS will become aware that an individual who is perceived to be a threat to aviation security and possibly a threat to national security was in a given airport at a given time.

As well, we are concerned that information from the PPP disclosed to law enforcement agencies in other countries could lead to very serious consequences for the individual affected—see below.

### 6.5 The Use of other "No-fly" Lists

Canadian carriers, as well as the carriers from other countries, may have access to the no-fly lists of other jurisdictions. We understand, for example, that a Canadian carrier flying to a United States destination is expected, or perhaps required, to screen passengers against the American no-fly list.

However, there does not appear to be anything to prevent a Canadian carrier from using an American no-fly list for flights to other destinations. We have been told by Transport Canada that it does not have the legal authority to prevent a Canadian carrier from using such a list.

The use of such lists causes concerns for several reasons:

- The PPP sets out procedures that individuals can follow if their names are on the SPL. These procedures are not ideal as discussed below but if carriers use other lists, these "appeal" processes will presumably not be available.
- The use of other lists may create confusion among travellers and further weaken their understanding of their rights.
- More fundamentally, the notion that a Canadian carrier might deny an individual the ability to fly within Canada based on information provided by a foreign government is inherently troubling.

The simplest way to deal with this problem would be for Transport Canada to use its licensing authority or any means at its disposal to prevent Canadian carriers from using other no-fly lists, with a possible exception for flights to destinations within the country providing the other list. Another approach would be to set out clearly the grounds under which a person can be denied boarding. In addition to an emergency direction issued under the PPP, carriers can apparently deny boarding to someone who is intoxicated or has a history of violent behaviour on an aircraft.[10]

### 6.6 Sharing of the Specified Persons List and other Personal Information with Foreign Governments

Section 9 of the Identity Screening Regulations addresses the issue of the confidentiality of the SPL:

> "no person shall disclose any information respecting the specified person that was provided to the air carrier by the Minister for the purposes of these Regulations including the specified person's name, date of birth, gender and the fact that he or she was specified.
>
> The air carrier shall ensure that access to information respecting the specified person is restricted to air carrier employees, agents or contractors who require that access to carry out their duties."[11]

This suggests that air carriers are required to keep the information in the SPL confidential. However, it is not clear how Transport Canada will monitor or prevent the possible disclosure of the SPL.

First of all, it is not apparent that Transport Canada would necessarily become aware that SPL has been shared with a foreign government. Secondly, in the case of foreign carriers, there would seem to be real possibility that faced with a court order or other legal instrument issued by a foreign court a carrier would be compelled to provide the SPL notwithstanding the confidentiality provision.

---

[10] On May 16, 2007, Transport Canada issued draft regulations under the authority of the *Aeronautics Act* to "establish procedures to prevent and manage incidents of interference with a crew member."

[11] See http://www.tc.gc.ca/acts-regulations/GENERAL/a/aa/regulations/290/aa291/aa291.htm

This issue was specifically addressed before the Commission of Inquiry on June 5, 2007. In response to a question from Raj Anand about the disclosure of the SPL by a foreign carrier to its national government, Mr. Brandt, from Transport Canada, stated:

> "And, you know, should their national government require that information of them, that's up to them to decide what they want to do with that information. We recognize that that possibility exists."[12]

The witnesses from Transport Canada went on to suggest that the Department had not considered making the confidentiality provision a condition of licence, i.e., that a carrier that disclosed this information to its national government would be prevented from operating in Canada. In other words, Transport Canada would not appear to have any effective method of enforcing the confidentiality provision.

The confidentiality provision does not address the sharing of the SPL with foreign government by Transport Canada. Transport Canada has not ruled out sharing the SPL with other governments as the following comments by Mr. Brandt suggests:

> "Well, as I mentioned that we haven't received a request from a foreign government to share the Specified Persons List, but one could envision that, you know, a country might request that we share that list with them.
>
> Not to speculate, but we would have to give that careful consideration in terms of if, you know, we are going to share information, for what purpose, and I think in the initial instant, the obligation would be on anyone who is interested in receiving that information to explain why.
> …
>
> And so we have no inclination to share it with other governments. If asked, we'd have to examine that situation.[13]

The sharing of the SPL with foreign governments is a concern for several reasons. First of all, the SPL is based on suspicion. The individuals on the SPL have not necessarily committed any crime. There is a significant risk that a foreign country would misinterpret the significance of the presence of the names on the list and take actions against someone on the list. Secondly, the SPL is not static; it will be updated or refreshed every 30 days. Names may be removed from the list based on new information or as a result of the reconsideration process. This is one of the positive aspects of the program but it highlights the risk that a foreign government may make use of an out of date list and take actions based on inaccurate information. Finally, while there are processes available in Canada to allow individuals to challenge the inclusion of their name on the SPL, these processes will not available in other jurisdictions.

As discussed below, foreign governments may become aware that an individual is on the SPL if an individual is denied boarding and is forced to seek assistance from his or her government.

---

[12] Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, Transcripts of Public Hearing, Volume 40, June 5, 2007, p.4912.

[13] Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182, Transcripts of Public Hearing, Volume 40, June 5, 2007, pp. 4880-4881.

### 6.7 The Consequences for Individuals Denied Boarding at the Airport

Once Transport Canada is satisfied that a person trying to board the aircraft is the person listed on the SPL the Minister of Transport can issue an Emergency Direction under sections 4.76 and 4.77 of the *Aeronautics Act* prohibiting the person from boarding the aircraft. As with the decision to add a name to the SPL, the decision to issue an Emergency Direction is made by the Minister, or his delegate, without any independent third party review.

According to section 4.771, the Emergency Direction ceases to have force after 72 hours. The obvious question that arises is what would happen if the same individual tried to board another flight after the 72 hours has expired. Would the Minister issue another Emergency Direction or would the individual be allowed to board the aircraft? If the former occurs, the 72 hour Emergency Direction becomes, in effect, a permanent ban, unless the individual can convince the Department that he or she should be de-listed. If the individual is allowed to fly one could ask why the person was prohibited from flying 72 hours previously. Transport Canada does not address this issue in the information provided on its web site.[14]

We have expressed concerns to Transport Canada about the way in which customer agents and airlines will deal with individuals who have been denied boarding. Other passengers may become aware if a passenger is not immediately given a boarding pass and is pulled aside for further questioning to determine if he or she is the person on the SPL. Other passengers may well make certain assumptions about the individual in question and this may be exacerbated if the individual is a member of visible minority.

Transport Canada has not adequately addressed the consequences for individuals who are denied boarding. It would seem that individuals who are denied boarding or who miss a flight have to deal with the airline to seek compensation.

The consequences of being denied boarding are potentially much greater in the case of international flights, for example, when someone departing Canada for a foreign country is denied boarding; or when someone is denied boarding in a foreign country.

A citizen of a foreign county who is denied boarding when attempting to return home from Canada would be in an almost impossible situation. The individual would not be able to stay in Canada but might not be able to find any alternative way of getting home. In this case the individual might end up contacting the country's representative in Canada. In order to explain the situation the individual would undoubtedly have to inform the representative that he or she is on Canada's SPL. This could subject the individual to additional scrutiny by his or her state. Similarly individuals denied boarding in a foreign country will be vulnerable and potentially at greater risk for detention.

Even more troubling is that local police forces, both in Canada and abroad, may be informed when an individual is denied boarding. According to Transport Canada, it notifies the RCMP immediately when an Emergency Direction has been issued, the RCMP notifies the local police and they can "take action as required."[15] In addition to notifying the local police, the RCMP will provide the specified person's name, gender, date of birth, and that there may be a breach of the peace.

---

[14] http://www.tc.gc.ca/vigilance/sep/passenger_protect/menu.htm
[15] *Ibid*.,

In the case of an international flight to Canada, the RCMP in Canada will inform the RCMP's International Liaison Branch in the departure country that an individual was denied boarding and a liaison officer could then inform the local police. We are concerned that this disclosure to law enforcement agencies in other countries could lead to very serious consequences for the individual affected.

At a minimum, this practice will make the local police aware that the individual in question is in a given country and city. More seriously, this information will make it easier for the local police force to monitor the individual's movements and it may lead to more serious consequences such as detention or deportation.

### 6.8 Redress: the Reconsideration Process

Individuals who have been denied boarding can apply to the Office of Reconsideration (OoR) for a review of their inclusion on the SPL. Individuals can attempt to make the case that their inclusion is a case of mistaken identity, i.e., I am not the John Smith in whom you are interested, or they can argue that they do not pose an immediate threat to aviation security.

In order to apply for a review, the applicant is required to submit a written application to the OoR outlining the grounds for reconsideration. The application must include authenticated copies of identity documents issued by a government and the application has to be validated by an official who has the authority to administer an oath or receive a solemn declaration, e.g. a lawyer or notary public.

The OoR will assess the application and recommend, based on an independent advisor's report, that the Minister of Transport either confirm the original decision or re-assess the file. According to the information on the Transport Canada web site[16] and in the Regulatory Impact Analysis Statement (RIAS) that accompanied the *Identity Screening Regulations*, individuals who wish to challenge the decision to uphold a listing on the SPL can seek a judicial review in Federal Court

There are several problems with this process:

- First of all, it will only assist those individuals who become aware that they are on the SPL;
- As discussed above, the criteria for adding individuals to the SPL are not clear which makes it difficult for individuals to challenge their inclusion;
- Although the application will be reviewed by an external advisor, the final decision will be made by the Minister or his delegate—the same person who made the initial determination to add the person to SPL and the same person who has the authority to issue an Emergency Direction prohibit the person from boarding the aircraft;
- There is no indication that individuals will have access to the information that has been used to justify their inclusion on the SPL; and
- This reconsideration process and more importantly, the right to seek a judicial review are not set out in either the *Identity Screening Regulations* or *the Aeronautics Act.*

[16] http://www.tc.gc.ca/Reconsideration/ppp/menu.htm and http://canadagazette.gc.ca/partII/2007/20070516/html/sor82-e.html

The reconsideration process might work better if individuals could learn in advance if they are on the SPL. This would allow individuals to clear up cases of mistaken identity prior to their flight and it would allow individuals on the SPL to explore other means of transportation. The RIAS accompanying the *Identity Screening Regulations* sets out three impediments to advance notification:

- For individuals not living in Canada, it would be difficult to locate and inform such persons;
- In cases where the background information is classified, or there is a warrant, it would not be possible to notify the individual; and
- The *Privacy Act* may also limit the information that could be disclosed, including information that was received from other agencies.

The RIAS goes on to suggest that "that by publishing the guidelines to be used for listing, the public will be well informed as to the reasons for being placed on the list."

These impediments to advance notification are not that convincing: the first assumes that Transport Canada would take the initiative to notify individuals. This rationale for not notifying is less compelling if individuals were allowed to initiate the inquiry. The second and third rationales seem to relate more to the information that could be released about why individuals are on the SPL rather than if they are on the list. As well, as discussed above, we question the claim that the guidelines would permit someone to determine if they are on the SPL and if so why they are on the list.

The issue of notifying individuals in advance and some of the reasons cited by Transport Canada why this is not possible raises an important concern common to other public safety and anti-terrorism measures about the ability of people who are suspected of wrongdoing or being a threat to obtain access to the incriminating evidence held by the state. This is a matter that should be addressed more comprehensively.

Allowing individuals to determine in advance if they are on the SPL may help some individuals in certain circumstances but it does not address the need for an effective, independent, legislatively-based adjudication process.

### 6.9 Oversight and Review

The Office of the Privacy Commissioner has the authority under the *Privacy Act* to audit any government program. The PPP will be high on our list of potential audit candidates. We also have the authority to investigate any complaints we may receive about the PPP. However, we believe there is a need for a specialized, independent review body or bodies to deal with public safety and national security programs. Effective oversight in this area is challenging and, based on our experience, would benefit from specific expertise.

In his "policy report", *A New Review Mechanism for the RCMP's National Security Activities*, that was issued as part of the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, Justice O'Connor recommended that the mandate of the Security Intelligence Review Committee (SIRC) be expanded to give it responsibility for the independent review of the national security activities of Citizenship and Immigration Canada (CIC), Transport Canada, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and

Foreign Affairs and International Trade Canada (DFAIT). SIRC would retain its current role of reviewing the activities of CSIS. He also recommended the creation of a new body, the Independent Complaints and National Security Review Agency, to review the RCMP and CBSA.

Justice O'Connor justifies this recommendation by referring to "the degree of integration of the national security activities of each of the five entities with those of the other federal actors subject to independent review, including the RCMP." He goes on to suggest that "Without the ability of an independent review body to make findings and recommendations about the five entities, there will be clear accountability gaps in the national security framework."[17]

With respect to Transport Canada, he notes that "Much of its work in this area takes place out of the public eye." He then states

> "Transport Canada's activities have the potential to affect individual rights, dignity and well-being to a significant extent. This is particularly so in the case of the security clearances it provides and the proposed creation of a no-fly list and passenger risk assessment program. Although the department has stated that it will create internal reconsideration mechanisms, none of these activities are currently subject to independent scrutiny."[18]

As Justice O'Connor notes in his report, the national security activities of CIC, Transport Canada, FINTRAC, DFAIT, CBSA, RCMP, CSIS and CSE are highly integrated. They share personal information among themselves and they take actions based on this information, actions that can have serious consequences for the individuals involved.

Other bodies have also called for greater oversight. In its report, *Fundamental Justice in Extraordinary Times*, on the *Anti-terrorism Act*, a Special Senate Committee recommended more effective oversight of the RCMP and it recommended the creation of a standing committee of the Senate, with dedicated staff and resources, to monitor, examine and periodically report on matters relating to Canada's anti-terrorism legislation and national security framework on an ongoing basis.[19]

To date, the government has not formally responded to these recommendations, although in its July 2007 response to the House of Commons Subcommittee on the review of the *Anti-terrorism Act*, it indicated it will develop a process for the review of national security activities consistent with Justice O'Connor's recommendations and it is considering an enhanced oversight role for Parliament.[20]

The passage of the *Anti-terrorism Act* and the *Public Safety Act* and the introduction of programs such as the PPP has created a new national security environment characterized by enhanced surveillance powers for law enforcement and national security agencies, a weakening

---

[17] Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, *A New Review Mechanism for the RCMP's National Security Activities,* pp. 561-562. See http://www.ararcommission.ca/eng/EnglishReportDec122006.pdf

[18] *Ibid*., pp. 566-567.

[19] *Fundamental Justice in Extraordinary Times: Main Report of the Special Senate Committee on the Anti-terrorism Act*, February 2007, Recommendations 38 and 39.

[20] Government of Canada, *Response of the Government of Canada to the Final Report of the Standing Committee on Public Safety and National Security Subcommittee on the Review of the Anti-Terrorism Act – Rights, Limits, Security: A Comprehensive Review of the Anti-Terrorism Act and Related Issues* (Ottawa, 2007), p. 25

of the constraints on the use of these powers and increased sharing of personal information within Canada and with foreign governments. We need independent oversight and review bodies that have the necessary authority and the expertise to ensure accountability and enhance transparency and we urge the government to act on the recommendations that have been made in this regard.

### 6.10 The Privacy Act and the Passenger Protect Program

The Commissioner's Resolution on the PPP notes that "The *Privacy Act* requires reform and offers no adequate protection or remedies to meet the privacy risks resulting from this type of initiatives."

In our June 2006 submission to the government "Government Accountability for Personal Information: Reforming the *Privacy Act*" we set out a number of reasons why the Act needs to be updated and we made a number of recommendations to reform the *Act*.[21] Although many of our recommendations are relevant to the PPP, the following are particularly critical not just to this program but to all public safety and national security measures.

1. Sharing of Personal Information with Foreign Governments

Paragraph 8(2)(f) of the *Privacy Act* authorizes disclosure of personal information under an agreement or arrangement between the government of Canada and the government of a foreign state.

This provision imposes only two duties on the disclosing institution: first, the disclosure must be made pursuant to an "agreement or arrangement"; second, the disclosure must be for the purposes of "administering or enforcing any law or carrying out a lawful investigation." The *Act* does not require the disclosing institution to identify the precise use of the information, apart from satisfying itself it will be used to administer a law. Nor is there any other obligation on the disclosing institution to ensure that personal information is treated confidentially by the foreign state.

The Treasury Board Secretariat has issued guidelines[22] that provide advice about what government institutions are required to do in order when disclosing personal information under paragraph 8(2)(f). These guidelines should be given the force of law within the *Act* or through regulations. As well, paragraph 8(2)(f) should be amended to state that personal information may only be disclosed where the information is required for the purpose of administering or enforcing any law which has a reasonable and direct connection to the original purpose for which the information was obtained.

2. Enhanced Court Review

---

[21] See http://www.privcom.gc.ca/information/pub/pa_reform_060605_e.asp

[22] Treasury Board Secretariat, *Privacy and Data Protection – Policies and Publications,* Chapter 2-4, pp. 7-8, section 6.6 (http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/dwnld/chap2_4_e.rtf) and Chapter 3-5 (http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_128/dwnld/chap3_5_e.rtf) (last accessed February 22, 2006).

The Privacy Commissioner can receive complaints concerning the full array of rights and protections under the *Privacy Act*, including complaints of inappropriate collection, use or disclosure, failure to maintain up-to-date and accurate data, improper retention or disposal, and complaints relating to denial of access or correction. Following an investigation, the Commissioner can make recommendations to the government institution and request notification of the actions it intends to take to correct any deficiency that is uncovered during the investigation.

However, if the institution does not accept the Commissioner's recommendations or its response is otherwise unsatisfactory, the Commissioner cannot go to the Federal Court to require the government institution to remedy its deficiencies. The Act only allows for Court review of a government institution's refusal to provide access to an individual's personal information. Neither the Court nor the Privacy Commissioner has any powers to provide a remedy as was confirmed recently in a decision by the Federal Court.[23]

Complainants, or the Commissioner acting on their behalf, should be able to ask the Court to review other matters dealing with the inappropriate or unlawful collection, use or disclosure of personal information following completion of an investigation. In addition, the Court should be empowered to assess damages against offending institutions.

3. A Comprehensive Accountability Framework for National Security Agencies

With the passage of the *Anti-terrorism Act* and the *Public Safety Act* and the introduction of measures such as the PPP and the API/PNR Program discussed above, the state and security agencies have been granted new powers to collect, use and disclose and, in some cases to withhold access to personal information.

However, we have not seen a corresponding increase in accountability. As we discuss elsewhere in this submission, there is a need for new and stronger oversight and review bodies. However, departments and agencies should also be required to develop stronger internal processes and procedures to protect the personal information they hold and to demonstrate accountability. This should include implementing internal privacy management frameworks, creating an internal privacy audit capacity and clearly defining accountability and privacy leadership responsibilities for the head of the institution. The Government of Canada and Parliament should consider amending the *Privacy Act* to ensure greater transparency, accountability and oversight over the departments and agencies involved in national security, including more stringent reporting requirements to Parliament. As we state in our submission on the reform of the *Privacy Act*:

> "In other words, the proportionality principle should apply here: with heightened powers to collect, use, disclose, process, share and aggregate personal information about the citizens and residents of Canada, the government of Canada needs to meet higher standards of accountability and answerability of public officials to Parliament."

## 7. Conclusion

Canada introduced several new programs to enhance aviation security, and made changes to existing programs, in the wake of the Air India bombing and more recently following the terrorist

[23] *Murdoch v. Canada (Royal Canadian Mounted Police),* [2005] 4 F.C.R. 340. 2005 FC 420

attacks of September 11, 2001. As discussed above, many of these programs involve the collection, use and disclosure of personal information or otherwise raise privacy concerns, for example because of the possibility of intrusive bodily searches.

The programs discussed in this submission include trusted traveler programs such as CANPASS Air and NEXUS that allow prescreened individuals to clear customs and immigration more quickly; the enhanced screening of certain airport workers and the use of biometrics to authenticate their identity; and the prescreening of passengers and their baggage.

Two other programs—the collection of Advance Passenger Information and Passenger Name Record (API/PNR) information and the Passenger Protect Program (PPP)—raise even more significant privacy concerns. Although aviation security is a worldwide concern, we find it noteworthy that, as far as we are aware, Canada and the United States are the only two countries that have considered it necessary to introduce both of these programs.

When the API/PNR program was initially proposed our Office raised several concerns about the creation of a database holding extensive information about the foreign travel of all law-abiding Canadians that could be shared widely and used for a virtually unlimited range of governmental and law enforcement purposes. Some of our concerns were addressed, for example, by shortening the period of retention and by limiting the purposes for which the information could be used. Further changes were made in response to pressure from the European Commission. Nonetheless, the collection and retention of a significant amount of personal information about all air travellers entering Canada is inherently troubling.

The PPP (the “no-fly list”) was implemented in June 2007. Under this program the Minister of Transport has the authority to issue an emergency declaration preventing individuals on a Specified Persons List (SPL) from boarding an aircraft on the grounds that they are an immediate threat to aviation security.

Our concerns about the PPP can be grouped into three broad categories

1. The Legislative Basis for the PPP

   The legislative basis for the PPP is found in a series of provisions in the *Aeronautics Act* that were added to the *Act* as a result of the passage of the *Public Safety Act* in 2004. However, during the two and a half year period when the Public Safety Act was being debated, the possibility that these provisions would be used to introduce a no-fly program does not appear to have been discussed publicly. As a result, neither Parliament nor the public had a meaningful opportunity to question or challenge the legislative basis for the PPP.

   In addition, many of the details of the program, such as the criteria that are used when adding individuals to the SPL and the reconsideration process, are not set out in the authorizing legislation or even in the *Identity Screening Regulations*. This means, for example, that these details can be changed without notice, Parliamentary scrutiny or public input.

2. The Design and Rationale of the Program

   The rationale for the program is not clear making it difficult for our Office to assess whether it is necessary or likely to be effective. While we support the desire to improve

aviation security we do not understand how forcing all travellers to identify themselves will necessarily deter those individuals who are determined to harm their fellow travelers.

More generally, this growing emphasis on identity screening creates the potential for increased monitoring and surveillance as more as more agencies collect more personal information about our travelling patterns. Increased identity screening may also lead to more intrusive authentication procedures or increase the pressure for a universal form of identification such as a national identity card.

We have questions about the creation of the SPL, the list of people who are prohibited from flying, including the criteria that will be used to identify individuals who may pose an immediate threat to aviation security and the role of the RCMP and CSIS in the creation of the SPL.

The reconsideration process is not built into the program nor is it independent. The final decision on applications will be made by the Minister—the same person responsible for adding the name to the SPL.

3. The Operation of the Program

The consequences for people denied boarding could be very serious, particularly in the case of flights to or from Canada. Individuals could effectively be forced to reveal to others that they are on the list. The consequences for individuals denied boarding could be even greater if the RCMP inform local police forces when an individual is denied boarding.

Transport Canada has not ruled out sharing the SPL with foreign government and even if it decides not to share the SPL there are other ways that foreign governments and law enforcement agencies may obtain the list or become aware that individuals are on the list. This creates significant risks for the residents of these countries or even people travelling to these countries who are on the SPL. Foreign government may well decide that individuals on the SPL should be subjected to surveillance, detention, or worse.

The inability or unwillingness of Transport Canada to prevent carriers from using the no-fly lists of other countries may create confusion among travellers and further weaken their understanding of their rights since the reconsideration processes that are available with the SPL will presumably not be available with respect to other lists.

These concerns prompted our Office, along with our provincial and territorial colleagues, to issue a joint resolution calling on the Government of Canada to suspend the program until a Parliamentary Committee was given the opportunity to review the justification and potential effectiveness of the program; the use of the no-fly lists of other countries; the impact on fundamental rights and freedoms; and the adequacy of the legal framework underlying the program.

Since it would now appear the government is unlikely to act on this recommendation,[24] it is all the more important that the government create an accessible, independent, adjudication process to ensure that individuals have a clear legal right to challenge listing decisions. Individuals should have a statutory right to appeal to an independent adjudicator or tribunal; they should be given an opportunity to challenge the information used to support the listing decision; and they should have the ability to seek redress including compensation. Equally important, the government should give a new or existing oversight and review body the duty to review and report on the operation of the program on a regular basis.

Canadians expect the government to take measures to protect them; equally, they expect that these measures will respect their rights, including their right to privacy, and conform to the rule of law. In assessing the adequacy of the measures currently in place to make air travel safer and before recommending new measures, we would urge the Commission of Inquiry to take into account the need for clear legal remedies, enforceable safeguards, and effective oversight to ensure that the rights of Canadians are protected.

[24] Following the release of the Resolution, Transport Canada issued a Press release in which the Minister reiterated the government's commitment to the Passenger Protect program See - http://www.tc.gc.ca/mediaroom/releases/nat/2007/07-h131e.htm
.