Office of the Information
and Privacy Commissioner

 # 410, 9925 – 109 Street
Edmonton, Alberta
Canada, T5K 2J8
Tel: (780) 422-6860
Toll Free within Alberta: 310-0000
Fax: (780) 422-5682
Web: www.oipc.ab.ca
Email: generalinfo@oipc.ab.ca

October 11, 2002

The Honourable Elinor Caplan
Minister of National Revenue
555 Mackenzie Avenue
Ottawa, ON
K1A 0L5

Dear Minister Caplan:

Re: Canada Customs and Revenue Agency Air Traveller Surveillance Database ("CCRA Surveillance Database")

Over the last year my office has monitored federal initiatives to protect Canadians against terrorism. I have offered what I hope has been accepted as balanced commentary on the information and privacy dimensions of those initiatives.

I have read the September 26, 2002, correspondence of my federal colleague, George Radwanski, the Privacy Commissioner of Canada, expressing his grave concerns about the creation of the CCRA Surveillance Database, as well as your response to him. I have also read the supporting public letters of concern sent to you by Ann Cavoukian, the Information and Privacy Commissioner of Ontario, and David Loukidelis, the Information and Privacy Commissioner for British Columbia.

I concur with my colleagues. I am compelled to add another letter to the growing pile of correspondence expressing concern about this project.

The CCRA wants an enforcement database that will collect and store the personal data of every person entering Canada from a foreign destination by air travel. That data could be retained for six years. You indicated in your letter to Mr. Radwanski that during 2000-2001, Canada Customs processed over 111 million travelers entering the country. Simple math suggests the magnitude of the database you propose to create and maintain.

Canadian public-sector privacy legislation, whether federal or provincial, prohibits public bodies from collecting personal data simply because it may become useful at some later point in time. In that regard, Canadian privacy laws track the limitations on government action found in section 1 of the Charter. In my view, the CCRA Surveillance Database, swollen beyond the parameters of the original initiative, does not respect fundamental legal constraints on government action. It has gotten the privacy and security balance wrong.

The point I want to add is that getting the privacy/security balance wrong has adverse implications for the security of Canadians. A respected American information security expert, Bruce Schneier, has repeatedly said that broad surveillance--the indiscriminate collection of data in the hope that it will disclose evidence of a threat--is a mark of bad security. In the September 30, 2001 issue of *Cryptogram* devoted to dissecting the September 11 terrorist attacks and their aftermath, he wrote:

> There's a world of difference between intelligence data and intelligence information. In what I am sure is the mother of all investigations, [in the aftermath of September 11] the CIA, NSA, and FBI have uncovered all sorts of data from their files, data that clearly indicates that an attack was being planned. Maybe it even clearly indicates the nature of the attack, or the date. I'm sure lots of information is there, in files, intercepts, computer memory.
>
> Armed with the clarity of hindsight, it's easy to look at all the data and point to what's important and relevant. It's even easy to take all that important and relevant data and turn it into information. And it's real easy to take that information and construct a picture of what's going on.
>
> It's a lot harder to do before the fact. Most data is irrelevant, and most leads are false ones. How does anyone know which is the important one, that effort should be spent on this specific threat and not the thousands of others?
>
> So much data is collected … that we can't possibly analyze it all. Imagine terrorists are hiding plans for attacks in the text of books in a large university library; you have no idea how many plans there are or where they are, and the library expands faster than you can possibly read it. Deciding what to look at is an impossible task, so a lot of good intelligence goes unlearned.
>
> Over the past couple of decades, the U.S. has relied more and more on high-tech electronic eavesdropping … and less and less on old fashioned human intelligence … . This only makes the analysis problem worse: too much data to look at, and not enough real-world context. Look at the

> intelligence failures of the past few years: failing to predict India's nuclear test, or the attack on the USS Cole, or the bombing of the two American embassies in Africa; concentrating on Wen Ho Lee to the exclusion of the real spies, like Robert Hanssen.

The vulnerability of a mammoth database such as the CCRA Surveillance Database is that it could be rendered useless by persons using aliases, false identity papers, and circuitous travel plans. Even worse, Schneier's analysis suggests that such a database could be used against itself to generate false leads and help hide real threats to Canadians.

I appreciate that you and the CCRA have the safety of Canadians at heart. I respectfully urge you to reconsider the CCRA Surveillance Database and revert to the earlier plan for a targeted and proportional approach to surveillance that was discussed with the Federal Privacy Commissioner.

Yours truly,

Frank J. Work, Q.C.
Information and Privacy Commissioner

Cc: George Radwanski, Privacy Commissioner of Canada
Provincial/Territorial Information and Privacy Commissioners