to their rights to privacy of their personal information in large data bases, even as technology for on line access and computer-based services becomes widespread and accepted. Even today consumers happily read out credit card data over the telephone to mail-order shops, but resent the use of this data for subsequent junk mail and even marketing based on the credit ratings determined as a result.

In the case of passport data, privacy of much of the information will remain an issue, in all liklihood preventing sharing and copying of data files and implying security for any access privileges granted to other agencies. However, in terms of biometric data (picture, signature, birthdate, fingerprint ?), the question can be raised regarding the violation of privacy, if any, that would be caused by permitting access to this data to authenticate a passport presented by the bearer at an Immigration point (Canada, USA, etc.). It must be borne in mind that the bearer is already voluntarily revealing this data to Immigration officers, since it is contained in the passport itself. If the Immigration officer calls up a display of file picture and signature for the bearer, it may not be realistic to claim that the display of equivalent biometric data from central files is a statute violation of privacy.

In the case that privacy statutes nonetheless restrict such biometric file access, the PPO may seek out an early implementation of the passport chip technology mentioned previously. This chip would store authentication information to confirm the data on the passport in which it is contained, and also contain certain control codes. The authentication process would involve verification of passport data by local checking of the authentication information with secure algorithms, followed if necessary by verification of the control codes centrally. These steps would not violate privacy of personal passport data files.

These issues of privacy could be resolved by requesting all applicants to sign a limited waiver for the release of such information in those circumstances as a way of ensuring no liability for subsequent action. The results of strategic planning for the 90's by the PPO should resolve this question into consideration and perhaps result in the implementation of such measures for all data collected as soon as possible, in order to build information banks of accessible passport data prior to these new systems being installed. The time period for construction of a complete new set of passport files (of current holders) is 5 years.