Guarantor lists could be automatically checked and a digitized signature of the guarantor could be automatically brought to the screen for on-the-spot comparison; guarantor statistics could be updated for off-line or back-ground analysis. Similarly, links to vital statistics registries might be automatically utilized to check the veracity of each application.

Digitized copies of complete previous application forms and supporting documentation might be available for recall by the Security section. (Similarly, complete digitized forms could be maintained for Certificate of Identity and Refugee Travel Document processing.) Direct links to FOSS, CPIC, PERS and other police systems might enable Security to perform more thorough checks. Data base searches by any data field could be possible - e.g. by address, by guarantor name, etc. - to allow analysis for security purposes.

The passport page could be printed with a digitized colour image, digitized signature, and digitized fingerprint; an imbedded chip (Write Once Read Many - "WORM") could also be written with the same biometrics and a polynomial checksum; the entire data/chip page would be laminated as it is presently.

If the application has been handled at a regional, local or overseas post, the above scenario could be identical in all respects, but checking of PCL lists, guarantor lists and other security data bases would be done remotely via telecommunication links to Ottawa. Any alarms or questionable applications might cause the entire application to be transmitted to Ottawa for Security or Adjudication personnel to handle.

After the application is processed all data might be automatically archived on optical disk. Applications could be automatically transmitted from remote sites for archiving.